ALESSANDRO FERREIRA DE ALBUQUERQUE

ESTUDO DE MÉTODOS DE PROTEÇÃO DE REDES WIRELESS

MEDIANEIRA – PR

2008

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ – UTFPR
CAMPUS MEDIANEIRA

ESTUDO DE MÉTODOS DE PROTEÇÃO DE REDES WIRELESS

ALESSANDRO FERREIRA DE ALBUQUERQUE

Monografia apresentada como requisito parcial ao Curso de Pós-Graduação *Lato-Senso* em Redes de Computadores – Configuração e Gerenciamento de Ativos, UTFPR – Universidade Tecnológica Federal do Paraná, Campus Medianeira.
Orientador: Hermano Pereira.

MEDIANEIRA – PR
2008

ESTUDO DE MÉTODOS DE PROTEÇÃO DE REDES WIRELESS

Alessandro Ferreira de Albuquerque

Este exemplar corresponde à redação final da monografia apresentada como requisito parcial para obtenção do grau de Especialista em Informática, Curso de Pós-Graduação em Redes de Computadores – Configuração e Gerenciamento de Ativos, UTFPR – Universidade Tecnológica Federal do Paraná, Campus Medianeira, aprovada pela comissão formada pelos professores:

Orientador: Hermano Pereira

Componentes da Banca: ____

Ms.C. Neylor Michel

____

Ms.C. Paulo Lopes de Menezes

Local e data de Aprovação: Medianeira, 15 de Março de 2008.

"Dominar-se a si próprio é uma vitória maior do que vencer a milhares em uma batalha."

Sakayamuni

DEDICATÓRIA

Aos meus pais Alberto e
Neuza pelo carinho e afeto
imenso com o qual me acolhem
nesta grande fase de minha
vida;

A minha querida e adorável
noiva Neuza Correia pelo
companheirismo em todos os
momentos;

Aos meus amigos e colegas
que juntos caminhamos e
lutamos até o final;

E a Deus, pai te todos, que possa nos
iluminar sempre com sua glória divina.

AGRADECIMENTOS

A minha noiva **Neuza Correia da Silva**, que me mostrou que a vida não somente é feita de materiais sólidos, e sim de momentos que podemos desfrutar hoje, sem deixarmos de aprender com os erros e viver cada momento que está se passando.

Aos meus pais **Alberto Ferreira de Albuquerque e Neuza de Fátima Squinzani Albuquerque**, que sempre me incentivaram para que eu pudesse almejar e alcançar meus sonhos, sempre com persistência e sem desistir, aprendendo com os erros e sempre buscando ver um objetivo de vida como uma grande conquista.

Aos meus irmãos **Francisney Ferreira de Albuquerque e Franciely Ferreira de Albuquerque**, que estavam sempre ao meu lado, dizendo palavras de conforto nos momentos difíceis e ajudando a compreender que a vida não é tão somente feita de palavras, e sim também de atos, que possam marcar pra sempre um simples acontecimento em nossas vidas.

Ao meu professor orientador e especialista **Hermano Pereira**, pela dedicação e competente orientação que fizeram com que seus conhecimentos enriquecessem este trabalho.

Aos professores **Alex Galvão, Antonio da Silva, Fernando Schutz, Neylor Michel e Olavo José Junior**, que sempre me orientaram no desenvolvimento deste trabalho, mostrando com evidência o caminho a ser percorrido para que eu pudesse atingir este objetivo com êxito.

A Universidade Tecnológica Federal do Paraná e Corpo Docente do curso de Pós Graduação em Redes de Computadores – Configuração de Ativos que puderam com seus grandes conhecimentos aumentar meu conhecimento profissional, tecnológico, científico e cultural.

RESUMO

A utilização do padrão 802.11 em redes locais sem fio, mais conhecidas como WLANs (Wireless Local Area Networks), vem crescendo consideravelmente nos dias atuais, pois empresas e instituições buscam sempre diminuir gastos em todos os seus setores. Com isto, o estudo de instalação de uma rede sem fio é bastante requisitado por possibilitar um ganho em economia de infra-estrutura de cabeamento, em mobilidade e em flexibilidade no acesso. Porém, com a utilização desse tipo de rede é necessário que algumas políticas de segurança sejam mais rígidas e explicitas e requerem um conhecimento significativo na tecnologia.

Sendo assim este trabalho tem por objetivo estudar e avaliar métodos seguros para as tecnologias existentes de redes sem fio para possibilitar uma implementação ou adequada em redes de pequenas e médias empresas. Para isso será feito um estudo sobre protocolos com suas respectivas vantagens e desvantagens de utilização, buscando obter segurança e a integridade das informações que trafegam na rede.

Contudo serão apresentados os conhecimentos adquiridos dos principais riscos e vulnerabilidades dos protocolos, mecanismos de segurança e dispositivos para redes sem fio, tipos de ataques e métodos utilizados para proteção das redes.

Ao final do estudo das tecnologias existentes, da análise dos riscos, vulnerabilidades e mecanismos de segurança, chegou-se a conclusão que em uma rede sem fio nunca estará totalmente segura, porém medidas são tomadas para tentar impedir ao máximo a ação de invasores.

Palavras chaves: Wireless, Wi-fi, Segurança de Redes Sem Fio.

ABSTRACT

The use of standard 802,11 in local nets without wire, more known as WLANs (Local Wireless Area Networks), comes considerably growing in the current days, therefore companies and institutions always search to diminish expenses in all its sectors. With this, the study of installation of a net without wire sufficiently she is requested by making possible a profit in cable infrastructure economy, mobility and flexibility in the access. However, with the use of this type of net it is necessary that some security politics are more rigid and explicitas and require a significant knowledge in the technology.

Being thus this work she has for objective to study and to evaluate safe methods for the existing technologies of nets without wire to make possible an adequate implementation or in average small nets of e companies. For this she will be made a study on protocols with its respective advantages and disadvantages of use, searching to get security and the integrity of the information that pass through in the net.

However the acquired knowledge of the main risks and vulnerabilities of the protocols, mechanisms of security and devices for nets without wire, types of attacks and methods used for protection of the nets will be presented.

At the end of the study of the existing technologies, of the analysis of the risks, vulnerabilities and mechanisms of security, it was arrived conclusion that in a net without wire never will be total insurance, however measured is taken to try to hinder to the maximum the action of invaders.

Words keys: Wireless, Wi-Fi, Security of Wi-fi.

SUMÁRIO

LISTA DE ABREVIATURAS

FHSS	*Frequency Hopping Spread Spectrum*
DSSS	*Direct Sequence Spread Spectrum*
Mbps	Megabits por segundo
WLAN	*Wireless Local Area Networks*
IEEE	*Institute of Electrical and Electronics Engineers*
WPAN	*Wireless Personal Area Networks*
Wi-Fi	Wireless Fidelity
WMAN	*Wireless Metropolitan Area Networks*
DSL	*Digital Subscriber Line*
AP	*Access Point*
GHz	Giga Herts
MHz	Mega Herts
WiMax	*Wireless Interoperability for Microwave Access*
WWiSE	*World Wide Spectrum Efficiency*
LAN	*Local Area Network*
EAP	*Extensible Authentication Protocol*
MAC	*Media Access Control*
OSI	*Open System Interconection*
LLC	*Logical Link Control*
HDLC	*High-level Data Link Control*
PCI	*Peripheral Component Interconnect*
POP	*Post Office Protocol*
SMTP	*Simple Mail Transfer Protocol*
SI	Sistemas de Informação
TI	Tecnologia da Informação
PGP	*Pretty Good Pricacy*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
WEP	*Wired Equivalent Privacy*
OUI	*Organizationally Unique Identifier*
WPA	*Wi-Fi Protected Access*

TKIP	*Temporal Key Integrity Protocol*
RADIUS	*Remote Authentication Dial-In User Service*
ICP	Infra-estrutura de Chaves Públicas
PKI	*Public Key Infrastructure*
IETF	*Internet Engineering Task Force*
ESP	*Encapsulated Security Payload*
AH	*Authentication Header*
IP	*Internet Protocol*
SSID	*Service Set IDentifier*
NMAP	*Network Mapper*
GPS	*Global Positioning System*
DoS	Denial os Service

LISTA DE FIGURAS

LISTA DE TABELAS

1. APRESENTAÇÃO

1.1. Introdução

A tecnologia de redes sem fio está crescendo notavelmente nos últimos anos, conquistando ambientes corporativos e domésticos. Sua característica de mobilidade torna flexíveis as alterações necessárias para suprir melhor as necessidades dos usuários. Além da mobilidade necessária, a segurança das informações que circulam na rede também é um ponto de elevada importância para estas empresas, necessitando assim de soluções mais adequadas. Veremos nos tópicos a seguir, uma explanação do cenário tecnológico atual, os objetivos do trabalho e como o mesmo é organizado.

1.2. Cenário Tecnológico

Em uma época, não muito distante, o conceito sobre rádio fazia parte do mundo do entretenimento, onde famílias se reuniam em volta de um aparelho de rádio do tamanho de uma cômoda para ouvirem as vozes que eram transmitidas de muito longe, e estas pessoas ficavam encantadas com a evolução da tecnologia, a ponto de permanecerem concentradas por horas sem sequer piscarem por minutos seguidos. As vozes e músicas chegavam sem a necessidade de fios entre o aparelho que estava transmitindo e o que estava recebendo. Essa tecnologia que encantava as pessoas de tempos passados, hoje está evoluída, pois a transmissão hoje não é somente de voz, a transmissão de dados tomou conta do espaço e se propaga cada vez mais. Ao invés de sinais de voz, transmitem uma seqüência de zeros e uns que são os tipos de informações que um computador processa. O tamanho do rádio também teve seu tamanho reduzido, em minúsculos micro-chips introduzidos dentro de um cartão de crédito, por exemplo (ENGST e FLEISHMAN, 2005).

1.3. Objetivos

1.3.1. Problema

Qual a melhor solução a ser aplicada em uma rede sem fio incorporada a uma rede cabeada, visando garantir a segurança, integridade e confiabilidade de ambas?

1.3.2. Objetivo Geral

O objetivo deste trabalho é desenvolver um estudo sobre segurança em tecnologias de redes sem fio, explorando suas vulnerabilidades e suas limitações, expondo o emprego ideal destas tecnologias para um ambiente corporativo, sendo este de pequeno ou médio porte, a fim de melhor atender suas necessidades e manter a integridade das informações que circulam em sua rede de informações.

1.3.3. Objetivos Específicos

- Pesquisar as novas tecnologias de redes sem fio;
- Pesquisar protocolos ou mecanismos de segurança em redes sem fio;
- Pesquisar e descrever os tipos de ataques em redes sem fios;
- Estudar ferramentas para administrar redes sem fio;
- Expor opções de soluções para implementação de uma rede sem fio em pequenas e médias empresas.

1.4. Motivação

A tecnologia de redes sem fio é nova e está surgindo fortemente, e com isso muitas vulnerabilidades podem ser encontradas. Existem muitas pessoas mal intencionadas e que se aproveitam das vulnerabilidades desta tecnologia e as exploram assiduamente, pois, em contrapartida, é difícil localizar de onde o invasor está atuando.

A necessidade de encontrar soluções apropriadas para implementação é, em muitos casos, prioridade no momento do planejamento de uma rede sem fio que irá se incorporar a uma cabeada. Na exploração dos meios e métodos utilizados na construção das redes sem fio podem ser encontradas muitas falhas e, a partir destas, propor soluções para minimizar ao máximo os riscos de ataques contra a rede.

1.5. Organização do Trabalho

Este trabalho está organizado em quatro capítulos, conforme segue:

No primeiro capítulo será feito uma introdução ao trabalho com breves informações sobre o assunto, explanando o que será abordado neste trabalho, justificando seu desenvolvimento, motivação e uma descrição de sua composição;

No segundo capítulo serão abordadas as tecnologias existentes para utilização em redes sem fio, bem como sua composição, funcionamento, aplicabilidade, padrões e definições;

O terceiro capítulo, a Segurança em Redes Sem Fio, é a parte principal deste trabalho onde serão descritos conceitos, tipos e formas de segurança existentes para redes sem fio. Serão propostas algumas formas de implementação de uma rede sem fio segura em um ambiente corporativo de pequeno e médio porte.

Finalizando o trabalho, no quarto capítulo serão feitas considerações finais com a conclusão do trabalho.

2. TECNOLOGIAS

2.1. Introdução

As redes de comunicações hoje possuem a função de interligar computadores. Com o avanço da tecnologia, surgiu a transmissão das informações de rede através de comunicação sem fio, para que se tenha uma maior flexibilidade e uma alta conectividade, proporcionando importantes avanços nesta área.

> *As redes sem fio consistem em redes de comunicações por enlaces sem fio como rádio freqüência e infravermelho que permitem mobilidade contínua através de sua área de abrangência. As redes sem fio são compostas por sistemas móveis, que têm como principal e mais difundido representante as redes celulares* (BEZERRA, 2004:23).

Nos tópicos seguintes, serão abordados assuntos referentes às definições de tecnologia sem fio, com uma explanação sobre o que são e como funcionam, seus modos de operação, padrões e tecnologias adotadas atualmente pelos fabricantes e desenvolvedores de sistemas. Ao final deste capítulo, alguns tipos de componentes serão apresentados como forma de exemplos para ilustrar a tecnologia utilizada no dias atuais.

2.2. Tipos de Transmissão

2.2.1. Radiofreqüência

Na comunicação utilizando radiofreqüência em redes locais com bandas não autorizadas, deve-se utilizar uma modulação do tipo *spread spectrum* adequando-o aos requerimentos para operação em vários países. Os padrões utilizados pela transmissão em radiofreqüência são o FHSS (*Frequency Hopping Spread Spectrum*) e o DSSS (*Direct Sequence Spread Spectrum*), e estes são definidos a utilizarem uma freqüência de 2.4 GHz (ZANETTI & GONÇALVES, 2003).

A tecnologia *spread spectrum* foi originalmente desenvolvida para uso militar. Sua função é distribuir o sinal uniformemente em toda a faixa de freqüência. A desvantagem desta utilização é o consumo grande da banda, porém garante a integridade das informações que nela trafegam e com isso diminui muito a sensibilidade a ruídos e a interferências de outros meios tecnológicos que possam estar utilizando a mesma freqüência para transmissão (RUFINO, 2005).

O FHSS utiliza uma banda de 2,4 GHz e está dividido em 75 canais e pode-se entender sua transmissão basicamente por efetuar um salto aleatório entre os canais para transmitir uma informação. Para que esta transmissão venha a ser completada com sucesso, o transmissor e o receptor devem estar sincronizados. Uma vez feito isso, ambos estabelecem um canal lógico. Portanto conclui-se que no FHSS o sinal é recebido somente por quem conhece a seqüência de saltos e para outros possíveis receptores aparece como sendo ruído. A velocidade de transmissão varia entre 1 e 2 Mbps (RUFINO, 2005).

O DSSS é utilizado pelo padrão 802.11b. A técnica utilizada pelo DSSS é denominada *code chips*, que nada mais é do que a separação de cada bit de dados em 11 bits, onde os mesmos são enviados de forma redundante pelo canal de comunicação. Este processo espalha a energia de rádio-freqüência em torno de uma banda larga que pode ser necessário para transmitir o dado. O DSSS torna-se mais vulnerável a ataques diretos e a ruídos que ocupam a banda de transmissão (RUFINO, 2005, ZANETTI & GONÇALVES, 2000).

2.2.2. Infravermelho

É uma tecnologia pouco utilizada para fins comerciais, pois trabalha em altas freqüências e transmissão direta dos dados, exigindo não possuir nenhum objeto entre o transmissor e o receptor, pois exige uma visada direta ou quase direta entre ambos. Tal camada física suporta duas taxas de dados: de 1 e 2 Mbps. Uma grande vantagem do infravermelho é que ele não sofre

interferências eletromagnéticas e nem de freqüências de rádio, tornando-o altamente seguro e impossibilitando que alguém possa interferir de qualquer modo no sinal. Esta tecnologia pode atingir em média um alcance de 1,5 metros (PALMELA & RODRIGUES, 2002).

Existem dois tipos de propagação do infravermelho: a direta e a difusa. Na propagação do sinal direto, como o próprio nome já diz, necessita de uma transmissão sem obstrução física entre as unidades que estejam trocando informações. Já na difusa, os transmissores emitem os sinais para uma superfície reflexiva, incluindo teto, paredes, piso, ou seja, todo o ambiente está repercutindo o sinal, eliminando assim a necessidade de alinhamento preciso com o receptor (ZANETTI & GONÇALVES, 2000).

2.2.3. Laser

A tecnologia laser é similar ao infravermelho, com a diferença de utilizar um comprimento de onda diferente. A transmissão laser é altamente direcional, ou seja, ambos os equipamentos de transmissão e recepção precisam obrigatoriamente estar alinhados para que se venha a ter uma comunicação completa, o contrário do infravermelho, que possui um ângulo de abertura. Uma vantagem que podemos considerar do laser sobre o infravermelho é o seu alcance que é superior, onde este é obtido conforme a potência aplicada no transmissor (TORRES, 2001).

2.3. Tipos de Rede Sem Fio

2.3.1. WLAN

As WLAN (*Wireless Local Area Networks*) são definidas pelo padrão IEEE (*Institute of Electrical and Electronics Engineers*) 802.11 (PERES & WEBER, 2004).

A WLAN é uma rede convencional, comparada a uma rede cabeada, pois oferece as mesmas funcionalidades, exceto por ter uma maior flexibilidade e conectividade em ambientes diversos, como escritórios, ambientes prediais entres outros. Sua composição é dada por transceptores (transmissores e receptores) os quais são estações clientes ligadas a pontos de acesso, e conseqüentemente estão diretamente ligados a uma rede cabeada ou a outros pontos de acesso (BEZERRA, 2004).

O desenho abaixo ilustra um exemplo de WLAN, onde existe uma rede cabeada possuindo computadores ligados diretamente a ela, e também um ponto de acesso para uma ligação de diversos computadores através de comunicação sem fio.

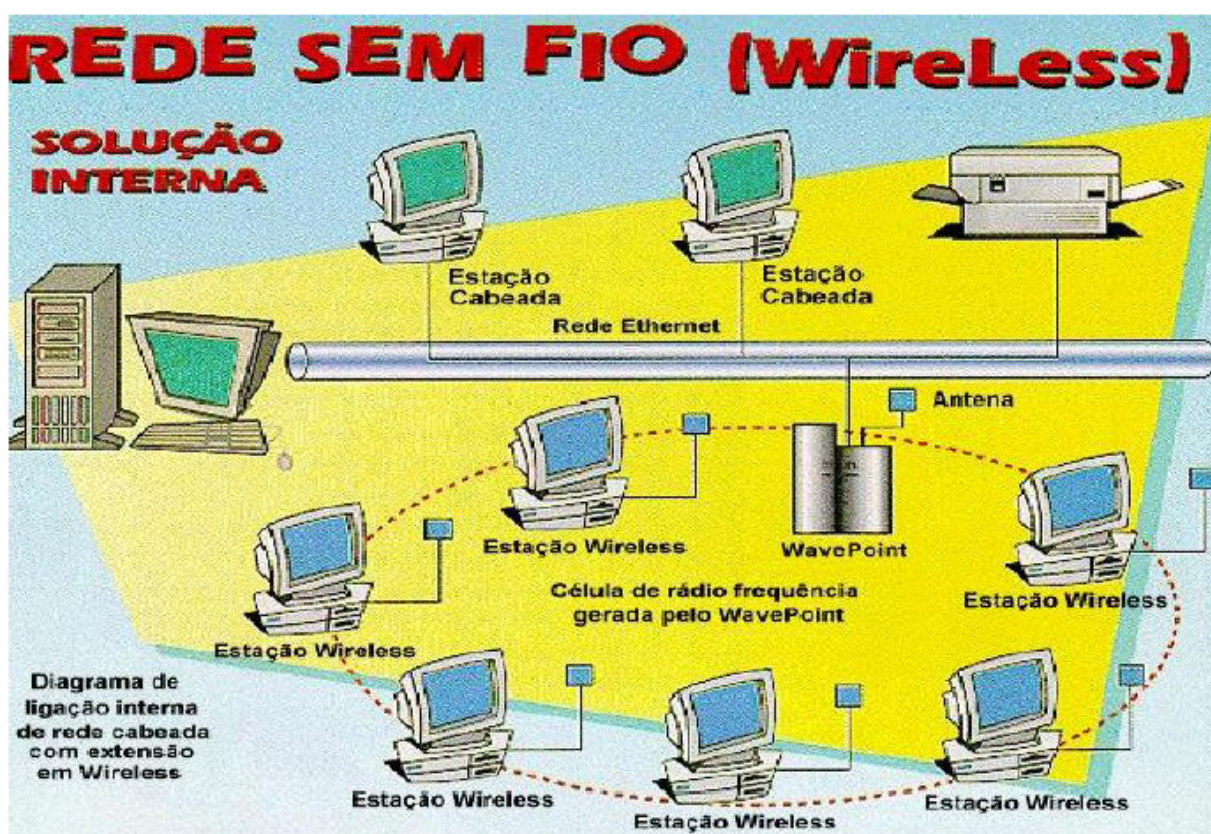



Figura 1 - Exemplo de WLAN (LOUREIRO et al., 2003).

2.3.2. WPAN

As WPAN (*Wireless Personal Area Networks)* são definidas pelo padrão *Bluetooth*, que atualmente é incorporado no padrão IEEE 802.15.

A tecnologia Bluetooth surgiu com os estudos na Ericsson Mobile Communication em meados do ano de 1994, com a finalidade de se criar uma transmisão de baixo custo e consumo entre celulares e seus acessórios. Em fevereiro de 1998 cinco empresas formaram um grupo chamado SIG (*Bluetooth Special Interest Group*), que era composto por Ericsson, Nokia, IBM, Toshiba e Intel e em maio do mesmo ano muitas outras empresas, como a 3COM e a Lucent, se juntaram para a criação da certificação para este novo padrão (ARAÚJO e ANDRADE, 2005).

Atualmente a utilização de Bluetooh é feita em celulares, palm tops, notebooks, microfones, fones de ouvidos, entre muitos outros dispositivos que visam facilitar o dia-a-dia do usuário.

O Bluetooth trabalha na freqüência de 2,45 Ghz (utilizada também pelos padrões 802.11b e 802.11g, que será visto nos próximos tópicos), e não é um substituto do Wi-Fi, pois a rede Bluetooth é mais lenta e possui poucos dispositivos suportados. Um destaque que pode ser dado para o Bluetooth é que o protocolo divide a faixa de freqüência em 79 canais e muda de canal 1600 vezes por segundo, isso é feito para evitar a interferência com outros protocolos.

A distância dos sinais emitidos pelo Bluetooth chega a aproximadamente 10 metros, uma distância curta comparada com outros protocolos (KOBAYASHI, 2004).

RUFINO (2005), diferentemente de KOBAYASHI (2004), afirma que as potências e os alcances podem variar em função de sua classe. Abaixo uma tabela explicativa das classes com suas respectivas potências e áreas de coberturas.

Classe	Potência Máxima (mW)	Potência Máxima (Dbm)	Área de Cobertura
Classe 1	100	20	100 metros ou mais
Classe 2	2,5	4	10 metros
Classe 3	1	0	11 metros

Tabela 1 – Potências e área de cobertura (RUFINO, 2005).

> *Dispositivos Bluetooth se comunicam entre si e formam uma rede denominada piconet, também chamada ad-hoc piconet. As piconets são redes locais com cobertura limitada e sem a necessidade de uma infraestrutura. Esse tipo de rede é importante para a conexão de diferentes pequenos dispositivos próximos uns dos outros sem a necessidade de infra-estrutura sem-fio* (ARAÚJO e ANDRADE, 2005:03).

O desenho abaixo ilustra um exemplo de uma rede WPAN.

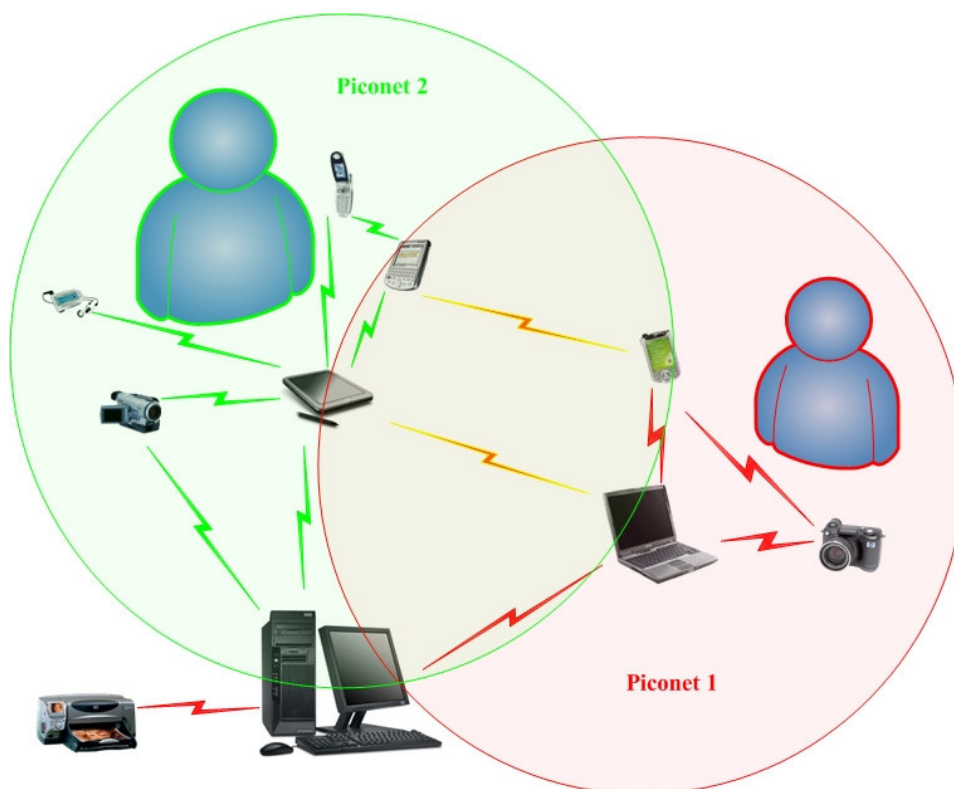



Figura 2 – Exemplo de WPAN (COMNETS, 2007).

2.3.3. WMAN

A WMAN (*Wireless Metropolitan Area Networks*) é definida pelo padrão IEEE 802.16 e também é conhecida como rede sem fio de banda larga. A WMAN é a principal concorrente da fibra óptica, pois possui como diferencial, devido sua grande mobilidade, alcance e disponibilidade que são serviços considerados superiores aos serviços de DSL (*Digital Subscriber Line* - Linha Digital para Assinantes) existentes, pois este possui uma limitação em sua distribuição relacionada a distâncias e custos (CAMARA & SILVA, 2005).

Seu funcionamento é bem similar ao sistema de rede celular, onde existem as estações bases localizadas próximas aos clientes que recebem o sinal (como as TV's via satélite), e depois disso fazem um roteamento através de uma conexão Ethernet padrão diretamente ligadas aos clientes (ONO, 2004).

O desenho abaixo ilustra um exemplo de várias redes interligadas, dando enfoque na ligação da WMAN com a internet.

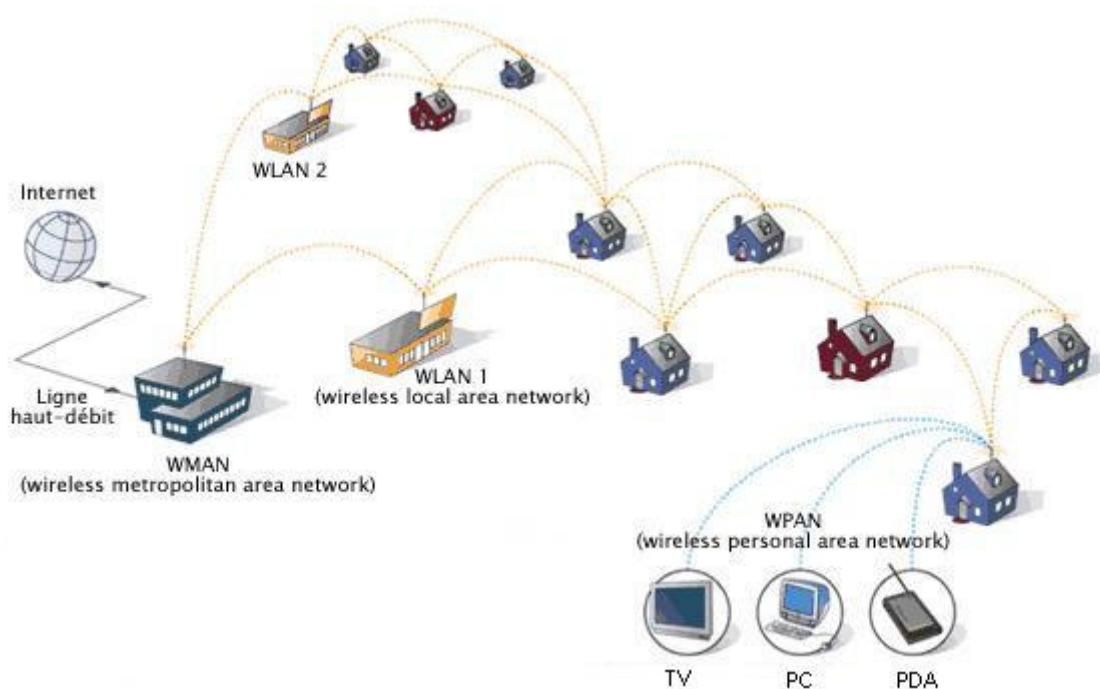



Figura 3 – Exemplo de WMAN (RENNES, 2007)

2.4. Modos de Operação

2.4.1. Redes Ad Hoc

Existe um modo de interligar computadores diretamente sem a utilização de um ponto de acesso (*Access Point*), e para esta ligação é dado o nome de "*ad hoc*", que é semelhante a uma ligação de um cabo cruzado (*crossover*) de Ethernet. Este tipo de conexão é inteiramente privado, onde um computador da rede se torna o controlador dela (ponto de acesso de software). É muito utilizado para a transferência de arquivos entre computadores na falta de outro meio. Apesar de ser um método para compartilhar arquivos pode também ser utilizado para compartilhamento de internet, através da configuração de um computador na rede, responsável pelo gerenciamento do compartilhamento (ENGST e FLEISHMAN, 2005).

Abaixo um exemplo simples de uma rede Ad Hoc.

Figura 4 – Rede Ad Hoc (ZANETTI & GONÇALVES, 2003).

2.4.2. Redes Infra-estruturadas

Uma rede infra-estruturada é composta por um AP (*Access Point* ou Ponto de Acesso) e clientes conectados a ele. O AP realiza um papel semelhante a um HUB ou roteador, fazendo assim uma ponte entre a rede cabeada e a rede sem fio. A ligação física entre ambas é feita de modo simples, bastando apenas conectar um cabo Ethernet da rede cabeada convencional ao ponto de acesso, onde este permitirá o acesso sem fio de seus clientes (ENGST E FLEISHMAN, 2005).

A figura a seguir demonstra um exemplo de ligação entre as redes.

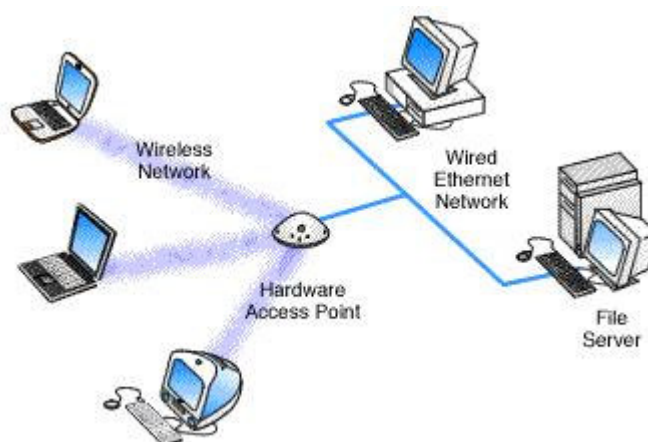



Figura 5 – Rede Cliente/Servidor utilizando um *Access Point.* (ZANETTI & GONÇALVES, 2003).

2.5. Padrões para Redes Sem fio

2.5.1. Introdução

ENGST e FLEISHMAN (2005), afirmam que no universo da tecnologia sem fio, existe uma padronização dos equipamentos de redes sem fio que funcionam conjuntamente, ou seja, equipamentos que suportam um dos padrões sempre são compatíveis com outros dispositivos que suportam o mesmo padrão. No mundo da tecnologia, esta padronização recebe um nome de especificação, que é aprovado por um órgão da indústria. O mais conhecido hoje é o IEEE (*Institute of Electrical and Electronics Engineers*).

O IEEE é uma associação profissional, cuja missão é desenvolver padrões técnicos com base no consenso de fabricantes, ou seja, definem como se dará a comunicação entre dispositivos clientes de rede. Com o passar dos tempos foram criados vários padrões, onde o que se destaca e melhor se desenvolveu foi o 802.11 (também conhecido como Wi-Fi - *Wireless Fidelity* – Fidelidade sem fio) (RUFINO, 2005).

Veremos a seguir as tecnologias mais comuns utilizadas pelas empresas no contexto atual, bem como algumas que ainda estão em fase de desenvolvimento.

2.5.2. Padrão 802.11b

Em meados de 1999 a 2001, surgiu o Padrão 802.11b, que hoje é chamado por ENGST e FLEISHMAN (2005), de "O Rei Dominante". Isso devido o motivo de ser o mais popular e com a maior base instalada com uma vasta gama de produtos e ferramentas de administração disponíveis no mercado atual. O 802.11b utiliza o espalhamento espectral por seqüência direta (DSSS) para receber e transmitir os dados a uma velocidade máxima de 11 megabits por segundo, porém esta não é sua velocidade real, pois estes 11 Mbps incluem todo o *overhead* (sobrecarga) de rede para o início e o fim dos pacotes. A taxa real pode variar de acordo com as configurações do equipamento e do espectro em que se encontra, porém pode variar entre 4 a 7 Mbps aproximadamente.

Este sub padrão do 802.11 opera na faixa de freqüência de 2.4 GHz e trabalha basicamente em cinco velocidades: 11Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps e 512 Kbps (variando entre 2,400 GHz a 2,4835 GHz aproximadamente), suportando no máximo 32 clientes conectados. (RUFINO, 2005).

Abaixo a tabela 02 demonstra seus canais com suas respectivas freqüências:

Canal	Freqüência
01	2,412
02	2,417
03	2,422
04	2,427
05	2,432
06	2,437
07	2,442
08	2,447
09	2,452
10	2,457

11	2,462
12	2,467
13	2,472
14	2,484

Tabela 2 – Associação entre canal e respectiva freqüência (RUFINO, 2005).

2.5.3. Padrão 802.11a

O padrão 802.11a é um padrão que trabalha na freqüência de 5 GHz, e surgiu em 1999, porém não é muito utilizado nos dias atuais, por não existirem muitos dispositivos fabricados que utilizem esta tecnologia (DUARTE, 2003). Os equipamentos do padrão 802.11a começaram a surgir em 2002, logo após o padrão 802.11b. Isso ocorreu porque o espectro em que o padrão 802.11a deveria operar ainda não estava disponível, bem como algumas tecnologias para seu desenvolvimento (ENGST e FLEISHMAN, 2005).

RUFINO (2005), ENGST e FLEISHMAN (2005) afirmam que as principais características do padrão 802.11a são as seguintes:

- O aumento de sua velocidade para utilização em 54 Mbps ou aproximadamente 25 Mbps de throughput real (108 Mbps em modo turbo), porém podendo ser utilizado para transmissões em velocidades mais baixas.

- Trabalha na faixa de 5 GHz, com pouquíssimos concorrentes, porém o alcance é reduzido, mas com melhores protocolos que o 802.11b.

- A quantidade de clientes conectados pode chegar a 64;

- Possui 12 canais não sobrepostos, que permite que os pontos de acessos possam cobrir a área um do outro sem causar interferências ou conflitos.

A sua principal desvantagem é a incompatibilidade com o padrão 802.11b, que já possui uma grande plataforma instalada no cenário tecnológico atual, pois ambos os padrões utilizam faixas de freqüências diferentes (ENGST e FLEISHMAN, 2005).

2.5.4. Padrão 802.11g

Surgiu em meados de 2002 como sendo a tecnologia que possui uma combinação ideal para utilização, a mais rápida e compatível no mercado de redes sem fio, pois trabalha com uma taxa de transferência de até 54 Mbps e na mesma freqüência do padrão 802.11b. Por existirem muitas divergências políticas para a adoção do 802.11a, o IEEE demorou mais de três anos para adotar definitivamente o padrão 802.11g, ocorrendo em 12 de junho de 2003 (ENGST e FLEISHMAN, 2005, RUFINO, 2005)

O padrão 802.11g pode se tornar um pouco mais lento que o 802.11a em uma mesma situação, mas isto é devido ao balanceamento de carga de transmissão com o 802.11b. Esta compatibilidade não é nenhum ponto opcional para o fabricante, ou seja, não cabe a ele determinar se no desenvolvimento de qualquer produto da linha 802.11g colocará uma compatibilidade com o 802.11b, este é uma parte obrigatória da especificação do padrão (ENGST e FLEISHMAN, 2005).

Suas principais características são:

- Velocidades que podem chegar a atingir 54 Mbps;
- Compatibilidade total com os equipamentos do protocolo 802.11b, pois ambos operam na freqüência de 2.4 GHz.

A figura a seguir mostra um exemplo de comunicação de uma rede sem fio nos padrões 802.11a ou 802.11g.

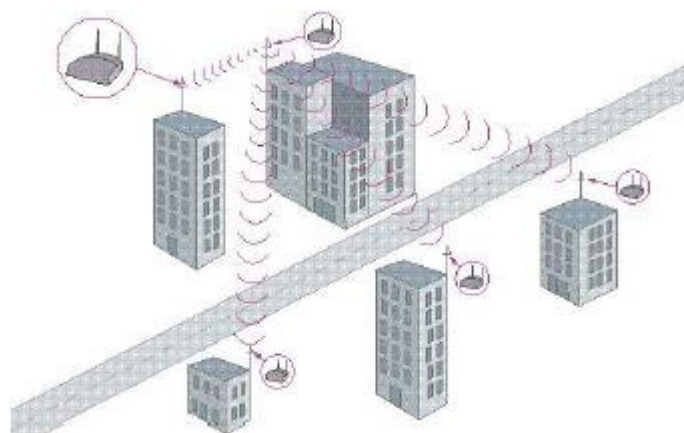



Figura 6 – Exemplo de Comunicação de redes 802.11a ou 802.11g (LOUREIRO et al., 2003).

2.5.5. Padrão 802.16 (WiMax)

Sua principal utilização e finalidade de criação é alcançar longas distâncias utilizando ondas de rádio, pois a utilização de cabos de rede para implementação de uma rede de dados de alta velocidade a uma distância longa, seja ela entre cidades, em uma residência ou em uma área rural, por exemplo, pode custar muito caro e estar ao alcance financeiro de poucos. Este padrão de rede se refere a uma WMAN, já citada em conceitos anteriores, que liga grandes distâncias em uma rede de banda larga. Visando desenvolver um padrão para atender esta demanda, o IEEE no seu papel de precursor da padronização, cria o padrão 802.16 (ENGST e FLEISHMAN, 2005).

Sua primeira especificação trabalhava na faixa de freqüência de 10 a 66 Ghz, ambas licenciadas como não licenciadas. Porém, com um pouco mais de trabalho surgiu recentemente o 802.16a, que abrange um intervalo de utilização compreendido entre 2 e 11 Ghz, incluindo assim a freqüência de 2,4 Ghz e 6 Ghz dos padrões 802.11b, 802.11g e 802.11a. A sigla utilizada para denominar o padrão 802.16 é o WiMax, que por sua vez, diferentemente de Wi-Fi, possui um significado real: *Wireless Interoperability for Microwave Access* (Interoperabilidade sem fio para acesso micro ondas), criado pela Intel e outras empresas líderes na fabricação de equipamentos e componentes de comunicação. A velocidade de transmissão de uma rede WiMax pode chegar

até 134,4 Mbps em bandas licenciadas e até 75 Mbps em redes não licenciadas. (ENGST e FLEISHMAN, 2005, CÂMARA e SILVA, 2005).

2.5.6. Padrão 802.11n

Este padrão ainda está em fase de definição tendo como sua principal finalidade o aumento da taxa de transmissão dos dados, algo próximo dos 100 a 500 Mbps. Este padrão também é conhecido como WWiSE (*World Wide Spectrum Efficiency*). Paralelamente objetiva-se alcançar um elevado aumento na área de cobertura do sinal. O padrão 802.1n pode operar com canais de 40 Mhz, e manter compatibilidade com os existentes atualmente que trabalham em 20 Mhz, porém suas velocidades oscilam em torno de135 Mbps (RUFINO, 2005).

2.5.7. Padrão 802.1x

Este tipo de padrão se refere a dois pontos de segurança fundamentais em uma rede sem fio, a Privacidade e a Autenticação. Na visão de autenticação, o padrão adota ao nível de porta, onde esta porta se refere a um ponto de conexão a uma LAN, podendo esta conexão ser física ou lógica (utilizando-se de dispositivos sem fio e AP). O padrão 802.1x surgiu para solucionar os problemas com a autenticação encontrados no 802.11. Sua implementação pode ser feita através de software ou de hardware, utilizando-se dispositivos específicos para esta função, oferecendo interoperabilidade e flexibilidade para a integração de componentes e funções (SILVA e DUARTE, 2005)

> *O padrão IEEE 802.1x especifica um mecanismo para autenticação de dispositivos e/ou usuários através da utilização de variações do protocolo EAP - Extensible Authentication Protocol. O protocolo EAP, na sua definição, permite a utilização de uma grande variedade de mecanismos de autenticação. A forma de funcionamento*

deste protocolo é baseada na troca de mensagens do tipo texto-desafio (PERES e WEBER, 2002:06*).*

Seu modo de funcionamento é bastante simples, porém eficiente. Consiste nada mais nada menos que colocar um "porteiro" para controlar o acesso à rede. Seu trabalho é evitar que indivíduos não autorizados acessem a rede, e para isso ele fornece credenciais aos clientes que podem ter acesso à mesma contendo um simples nome de usuário e uma senha ou um sistema de controle mais rigoroso que verifica a autenticidade de uma assinatura digital, por exemplo. Todo seu funcionamento é composto por três elementos: o cliente que pode ser chamado de solicitante, um ponto de acesso à rede que será responsável pela autenticação (o porteiro), e um servidor de autenticação, que conterá um banco de dados com as informações necessárias para a autenticação do cliente (ENGST e FLEISHMAN, 2005).

Portanto é simples de entender seu modo de autenticação. O cliente solicita a entrada na rede para o porteiro (ponto de acesso) e este por sua vez envia as informações recebidas do cliente até o servidor de autenticação, que retornará se as informações são válidas ou não. Caso as informações sejam corretas, o porteiro fornece o acesso à rede para o cliente que solicitou.

2.6. Arquitetura do protocolo 802.11

A arquitetura do protocolo 802.11 possui apenas algumas camadas diferentes do modelo de referência OSI (*Open System Interconection* - Interconexão de Sistemas Abertos). Podemos destacar a Camada Física, o Controle de Acesso ao Meio (MAC) e o Controle de Enlace Lógico (LLC). Na Camada Física e no Controle de Acesso ao meio, podemos ver, conforme ilustração abaixo, as diferenças entre diversos protocolos:

	802.3	802.4	802.5	802.6	802.11	802.12	802.16
MAC	CSMA/CD ethernet	Token bus	Token ring	DQDB	CSMA (WLAN)	prioridade	WLAN Banda Larga
Física	Coaxial Fios* Fibra	Coaxial Fibra	Fios*	Fibra	Sem fio	Fios*	Sem fio

* Par de fios trançados

Tabela 3 – Comparativo entre protocolos (TELECO, 2007).

No que diz respeito ao Controle de Enlace Lógico, podemos citar que: “A LLC especifica os mecanismos para endereçamento de estações conectadas ao meio e para controlar a troca de dados entre usuários da rede. A operação e formato deste padrão são baseados no protocolo HDLC (*High-level Data Link Control* – Controle de Ligação de Dados de Alto Nível). Estabelece três tipos de serviço: 1) sem conexão e sem reconhecimento, 2) com conexão e 3) com reconhecimento e sem conexão” (PRADO, 2005).

A figura abaixo mostra a posição do padrão IEEE 802.11 dentro do modelo OSI:

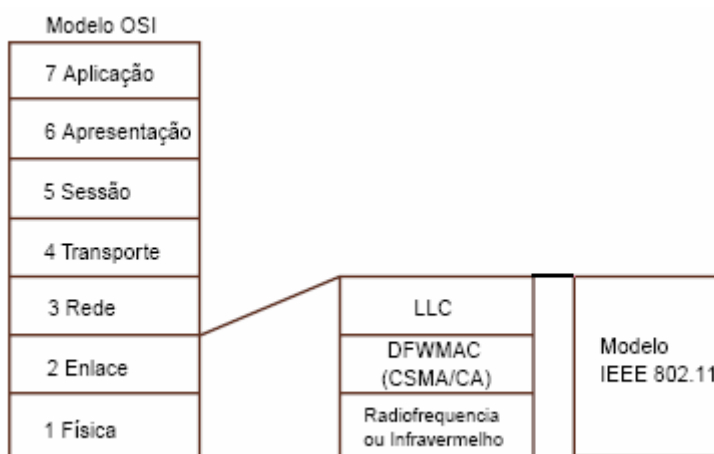



Figura 7 – Posição do IEEE 802.11 no modelo de referência OSI (JR. & SILVA, 2005).

No próximo tópico, citar-se-á exemplos de equipamentos que podem ser utilizados em uma rede sem fio, com uma breve explicação da aplicação de cada um deles.

2.7. Componentes de Redes Sem fio

Neste tópico serão explanados alguns dos equipamentos comumente utilizados para a comunicação de uma rede utilizando o meio de transporte de dados e voz através das ondas de rádio, conhecido como redes Wireless, conforme já foi mencionado em capítulos anteriores.

A figura abaixo exemplifica um Ponto de Acesso, onde equipamentos como computadores, Palm Tops, notebooks e outros, podem se conectar a ele para ter acesso a uma rede local, sendo ela cabeada ou não.

Figura 8 – Ponto de Acesso (TEXTUSWEB, 2007).

A figura seguinte mostra uma placa PCI (*Peripheral Component Interconnect* - Interconector de Componentes Periféricos) dotada de um chip rádio que normalmente é conectada internamente em um computador pessoal para comunicação com outros computadores em uma rede *Ad Hoc* ou a um Ponto de Acesso, para acesso a uma rede sem fio, ou até mesmo cabeada.

Figura 9 – Placa PCI WLAN (ABTRON, 2007).

Na figura seguinte é mostrada um exemplo de uma rede WPAN, onde vários dispositivos de rede se comunicam através da tecnologia Bluetooth.

Figura 10 – Dispositivos Bluetooth. (PCTUNING, 2007).

Nestas próximas figuras são apresentados dois exemplos de antenas externas que são utilizadas para comunicação a maiores distâncias. A figura da esquerda é um exemplo de antena omni-direcional que propaga seu sinal por todas as direções. A figura da direita é uma antena direcional, que como o

próprio nome já diz, propaga seu sinal em apenas uma direção, utilizada comumente para fechar a área de captação do sinal, diminuindo assim as chances de interceptações do mesmo.

Figura 11 - Exemplo de antena omni direcional (QADOMINICANA e IB, 2007).

Figura 12 - Exemplo de antena direcional (QADOMINICANA e IB, 2007).

No próximo capitulo serão abordadas várias formas de proteção a serem utilizadas em redes sem fio, tendo em vista que existem diversos métodos, onde os mesmos são utilizados de acordo com as necessidades do nível de segurança exigido. Métodos de invasão, riscos e vulnerabilidades serão citados apenas como forma de exemplificar as ações possíveis, com intuito benéfico pelos administradores e clientes de redes sem fio.

3. SEGURANÇA EM REDES SEM FIO

3.1. Mecanismos de Segurança

3.1.1. Cifragem e Autenticidade

A preocupação com os dados que trafegam em uma rede sem fio é uma questão muito discutida entre diversos profissionais da área. Apenas a restrição ao acesso à rede não é suficiente, é necessário também manter seguro os dados que nela trafegam.

A cifragem, também conhecida como **criptografia** (do Grego *kryptós*, "escondido", e *gráphein*, "escrever") pode ser entendida como um processo de transformação de uma informação de sua forma original para uma forma ilegível utilizando-se uma chave secreta. Para novamente, quando necessário, ter acesso ao conteúdo original, somente em posse desta chave poderá ser possível decifrar esta informação. (WIKIPÉDIA, 2007)

A autenticidade, seja ela de um usuário, informação ou serviço, é um método que permite um sistema ter a certeza de que o elemento que se está identificando é realmente quem diz ser. Normalmente este processo utiliza-se de um nome de usuário e de uma chave secreta (senha), que fica armazenado em uma base de dados o qual o autenticador fará a consulta para verificar se as informações estão corretas liberando assim o acesso às requisições solicitadas pelo elemento autenticado.

A utilização de métodos para a autenticação e cifragem de senhas dos diversos serviços que está sendo necessário é sugerido em situações que se utilizam, por exemplo, o correio eletrônico (utilização do APOP – *Authenticated Post Office Protocol*, e do SMTP AUTH – *Authenticated Simple Mail Transfer Protocol*), também na utilização no conteúdo (uso do PGP – *Pretty Good Pricacy* – Muito Boa Privacidade), em acesso remoto por SSH (*Secure Shell* – Shell Seguro) utilizando SSL (*Secure Sockets Layer*) como cifragem do mesmo, e também a grande conhecida VPN (*Virtual Private Network* – Rede Privada Virtual), que será vista em um tópico futuro (PERES & WEBER, 2005, ENGST e FLEISHMAN, 2005).

No próximo tópico, veremos a utilização de métodos e protocolos para garantir a segurança da rede como um todo, ou ao menos, diminuir ou dificultar o acesso indevido a mesma.

3.1.2. WEP

Para que se possa ter uma comunicação em uma rede sem fio, basta apenas ter um meio para recepção do sinal, ou seja, uma recepção passiva, diferentemente de uma rede cabeada, que necessita obrigatoriamente de uma conexão física entre os dois componentes de rede. Por esta razão, o protocolo 802.11 oferece uma opção de cifragem de dados, onde o protocolo WEP (*Wired Equivalent Privacy*) é sugerido como solução para o problema, que está totalmente disseminado e presente nos produtos que estão dentro dos padrões definidos pela IEEE para redes Wi-Fi (RUFINO, 2005).

O protocolo WEP trabalha na camada de enlace de dados e é baseada na criptografia do tipo RC4 da RSA, utilizando um vetor de inicialização (IV) de 24 bits e sua chave secreta é compartilhada em 104 bits, que depois de concatenada completam os 128 bits utilizados para a cifragem dos dados. Para que seja checada a integridade dos dados, o protocolo WEP do transmissor utiliza o CRC-32 para calcular o *checksum* da mensagem transmitida e o receptor faz o mesmo para checar se a mensagem não foi alterada. Existe ainda a possibilidade de o protocolo trabalhar com o padrão mais simples, de 64 bits onde a chave pode ser de 40 ou 24 bits, portanto o padrão de cifragem dos dados é diferente do padrão de 128 bits, garantindo assim duas opções de escolha para tentar obter um nível mínimo de segurança na rede (CANSIAN et al., 2004, AMARAL e MAESTRELLI, 2004).

A figura abaixo ilustra o processo de autenticação e cifragem do protocolo WEP.

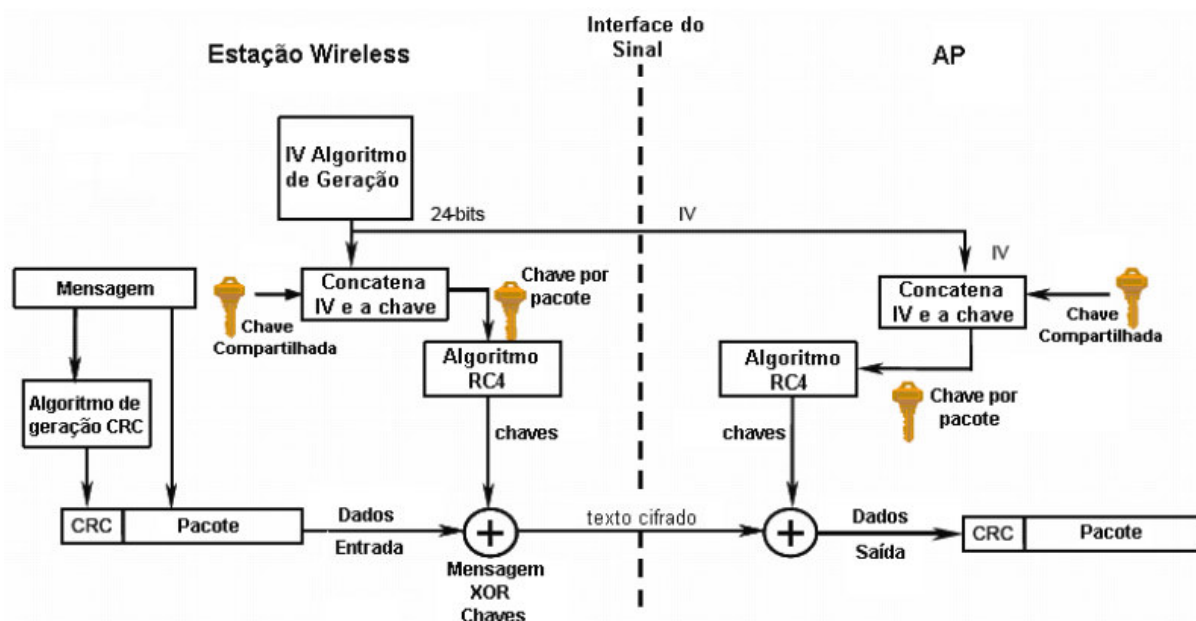



Figura 13 - Processo de autenticação do protocolo WEP (AMARAL e MAESTRELLI, 2004).

ENGST e FLEISHMAN (2005) descrevem o protocolo WEP com sendo uma porta trancada, impedindo que invasores consigam entrar na rede sem fio. Basicamente, o WEP cifra todos os dados que circulam na rede, impedindo a espionagem dos invasores. Sua fundamentação é a utilização de uma “chave segredo”, ou uma chave cifrada (pode ser até quatro por rede), que é compartilhada por todos na rede. Esta chave é introduzida manualmente por cada usuário da rede nos dispositivos que necessitam ter acesso à mesma que é protegida por WEP. Esta chave é utilizada na cifragem e decifragem das mensagens que circulam na rede sem fio, para garantir assim um nível considerado de segurança da mesma, porém é um pouco incômoda para o usuário, visto que esta é definida por um sistema hexadecimal de base 16, e a maioria dos usuários não faz idéia do que isso significa e nem como lidar com isso.

Apesar dos pontos negativos citados do protocolo WEP, sua utilização fornece um mínimo de segurança que é adequada em muitos cenários atuais. Em um capítulo posterior, verificaremos com maiores detalhes suas falhas e suas possíveis utilizações.

3.1.3. MAC

Para que uma rede funcione de maneira eficiente e eficaz, seja ela uma Ethernet ou Wi-Fi, cada dispositivo da rede deve possui uma identificação, para que o equipamento que esteja controlando a rede possa ter a capacidade de concretizar uma organização da mesma. Essa identificação foi definida pelo *Institute of Electrical and Electronics Engineers* (IEEE), como sendo um número único para cada dispositivo fabricado mundialmente, para evitar qualquer tipo de conflito ou colisão entre os mesmos (RUFINO, 2005).

O IEEE padronizou os endereços MAC em um quadro com seis bytes, onde os três primeiros identificam o fabricante do dispositivo, e os três últimos são para controle do próprio fabricante, sendo necessário seu cadastramento o IEEE para poder receber sua OUI (*Organizationally Unique Identifier*). Um mesmo fabricante pode ter mais de um OUI, evitando assim o problema de repetição dos números em caso de fabricação de dispositivos em grande escala (TORRES, 2001).

Uma das formas de prevenir uma entrada indevida, ou uma invasão em uma rede sem fio, é cadastrando o endereço MAC (*Media Access Control)* de cada dispositivo da rede no controlador da rede, que pode ser um roteador, um ponto de acesso, entre outros. Esse controlador da rede, só permitirá a entrada dos cadastrados em sua base de dados, ignorando outros que porventura possa tentar entrar em sua área de atuação (RUFINO, 2005).

3.1.4. WPA

O protocolo WPA (*Wi-Fi Protected Access*) também conhecido como WEP2 ou TKIP (*Temporal Key Integrity Protocol* - protocolo de chave temporária) surgiu para corrigir os problemas de segurança encontrados no WEP, e implementou a autenticação e a cifragem do trabalho que estava sendo desenvolvido em outros padrões baseados no 802.11. O WPA atua em duas áreas distintas: sua primeira atuação é a substituição total do WEP, ou seja, sua cifragem objetivando a integridade e a privacidade das informações

que trafegam na rede. A segunda área de atuação foca diretamente a autenticação do usuário utilizando uma troca de chaves dinâmica, que não era feita pelo WEP e, também, a substituição do vetor de inicialização de 24 bits do WEP para 48. Para isto o WPA utiliza as definições do padrão 802.1x já visto em tópicos anteriores, e o EAP (*Extensible Authentication Protocol* - Protocolo de Autenticação Extensível), que será visto ainda neste capítulo (RUFINO, 2005, CANSIAN et al., 2004).

SILVA (2005) afirma que "O WPA padronizou o uso do Michael, também conhecido como MIC (*Message Integrity Check*), em substituição ao CRC-32, melhorando a garantia da integridade dos dados em trânsito". Michael é uma função *hash* com criptografia chaveada, que produz uma saída de 64 bits. A segurança do Michael baseia-se no fato de que o valor do MIC é cifrado e desconhecido pelo atacante. O método do algoritmo de cifração do WPA é o mesmo utilizado pelo WEP, o RC4.

A figura abaixo, mostra um quadro comparativo entre o WEP e o WPA.

Característica de segurança	WEP	WPA
Algoritmos de cifração	RC4	RC4
Gerenciamento de chaves	nenhum	Baseado em EAP
Tamanho de chaves	40 ou 104 bits	128 bits (64 bits para autenticação)
Chave do pacote	criada por concatenação	criada por função de mistura
Integridade de dados/cabeçalho	CRC32/nenhum	MIC
Proteção contra reprodução	nenhuma	uso do VI

Tabela 4 – Quadro comparativo entre WEP e WPA (WOLSKI, 2003).

Nos próximos dois tópicos serão abordados com maior ênfase as principais mudanças na implementação do protocolo WPA com relação ao WEP.

3.1.4.1. Criptografia (Cifrar e Decifrar)

Esta parte do WPA foi uma das modificações feitas para a solução dos problemas de criptografia existentes no WEP utilizando a combinação entre o algoritmo e a temporalidade da chave.

A utilização da chave para cifrar é utilizada de forma distinta em ambientes distintos, como em um local doméstico onde será utilizada uma chave compartilhada previamente, conhecida como "Chave Master", onde esta será responsável pelo reconhecimento do dispositivo com o concentrador. A outra forma é a utilização em uma rede pequena, chamada de "Infra-estruturada", onde existirá um servidor RADIUS (*Remote Authentication Dial-In User Service* - Serviço de Autenticação de Usuários Discados) para que seja feita uma autenticação para acesso à rede. Poderá ainda este, necessitar de chaves públicas (ICP - Infra-estrutura de Chaves Públicas), no caso da utilização de certificados digitais para a autenticação dos usuários (RUFINO, 2005).

3.1.4.2. EAP

O EAP (*Extensible Authentication Protocol*) é um modelo ao qual foi desenvolvido para a autenticação no WPA, cuja sua finalidade é integrar as soluções de autenticação já existentes, conhecidas e testadas, como por exemplo, a autenticação utilizada em conexões discadas (RADIUS) permitindo inclusive a possibilidade de uma autenticação com certificação digital (RUFINO, 2005).

Seu funcionamento dá-se pela utilização e um serviço de autenticação, onde o autenticador recebe uma requisição de um suplicante (entidade que

está solicitando a autenticação) onde este se conecta a um servidor de autenticação abrindo uma porta específica para tal solicitação, não permitindo qualquer outro tipo de tráfego enquanto durar a autenticação. A figura abaixo mostra um modelo dos três elementos formadores (SILVA e DUARTE, 2005).

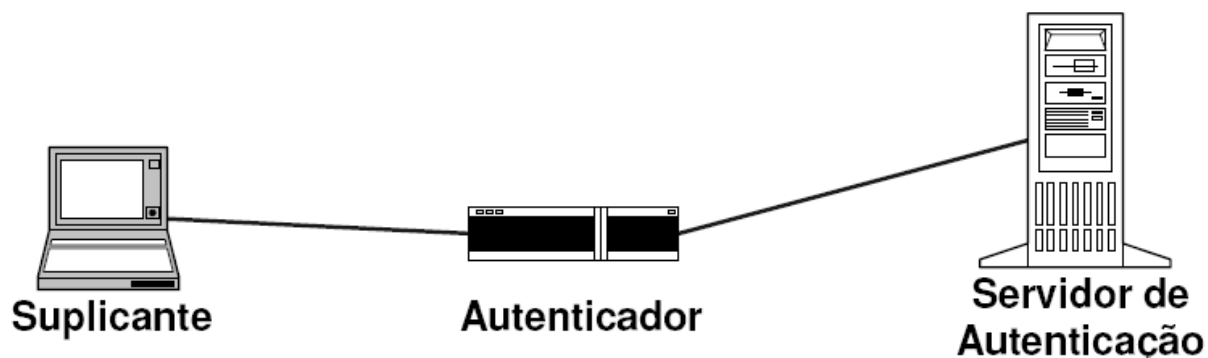



Figura 14 - Rede IEEE 802.11 / IEEE 802.1X (SILVA e DUARTE, 2005).

BOAVIDA (2004), AMARAL E MAESTRELLI (2004) afirmam que o EAP pode funcionar de cinco maneiras conforme descrito abaixo:

- MD5 → utiliza um método de autenticação simples utilizando *password*;

- LEAP (lightweight EAP) → este método é uma versão proprietária da CISCO, funcionando somente em equipamentos e softwares fabricados pela mesma e utiliza senhas para autenticar seus usuários;

- EAP-TLS → esta é uma normalização da IETF (*Internet Engineering Task Force* - organização responsável por especificar o desenvolvimento ou uso de protocolos e a melhor arquitetura para resolver problemas operacionais e técnicos na Internet) onde é feita uma autenticação mútua baseando-se em certificados PKI (Public Key Infrastructure - Infra-estrutura de chaves públicas);

- EAP-TTLS e PEAP → são similares ao tipo de autenticação EAP e são suportados por várias marcas de produtos WLAN. Estes protocolos utilizam certificados digitais assim como o EAP-TLS,

porém requerem autenticação apenas no servidor RADIUS. A estação autentica o servidor RADIUS e um túnel seguro é então estabelecido entre a estação e o servidor através do qual o servidor RADIUS poderá autenticar a estação.

3.1.5. VPN

O surgimento da VPN (*Virtual Private Network* – Rede Privada Virtual) se deu devido as grandes necessidades de empresas se comunicarem por meio de uma comunicação segura através de redes que não sejam tão confiáveis. As informações que trafegam em uma rede pública podem ser facilmente interceptadas por qualquer indivíduo com esta intenção e servirem de objetos para chantagem, manipulações e outros ilícitos do gênero (ROSSI & FRANZIN, 2000).

O custo de uma rede privada é muito elevado e com a evolução da internet possibilitando conexões em banda larga, surgiu a VPN através desta rede (que por sua vez é considerada uma rede pública), devido a seu baixo custo. A VPN é uma rede virtual dentro da internet, também é muito conhecida pelo conceito de criar um "túnel" dentro da internet para a comunicação de informações entre dois ou mais pontos de uma empresa, por exemplo. A sua principal característica é não permitir que nenhum tipo de informação fuja deste túnel criado para o tráfego das mesmas.

Abaixo podemos ver dois exemplos de conexão VPN:

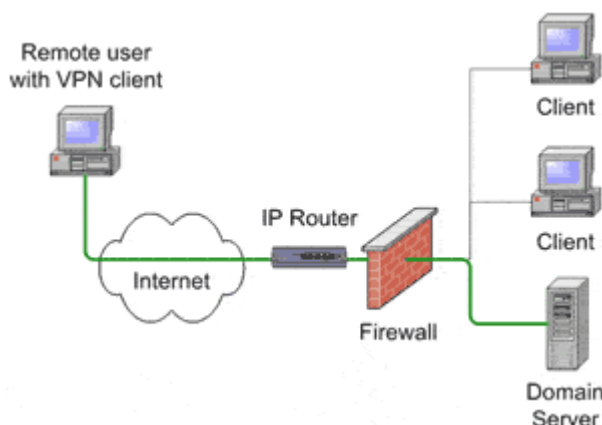



Figura 15 – Ilustração de uma conexão VPN simples (NEOMEDIA, 2007).

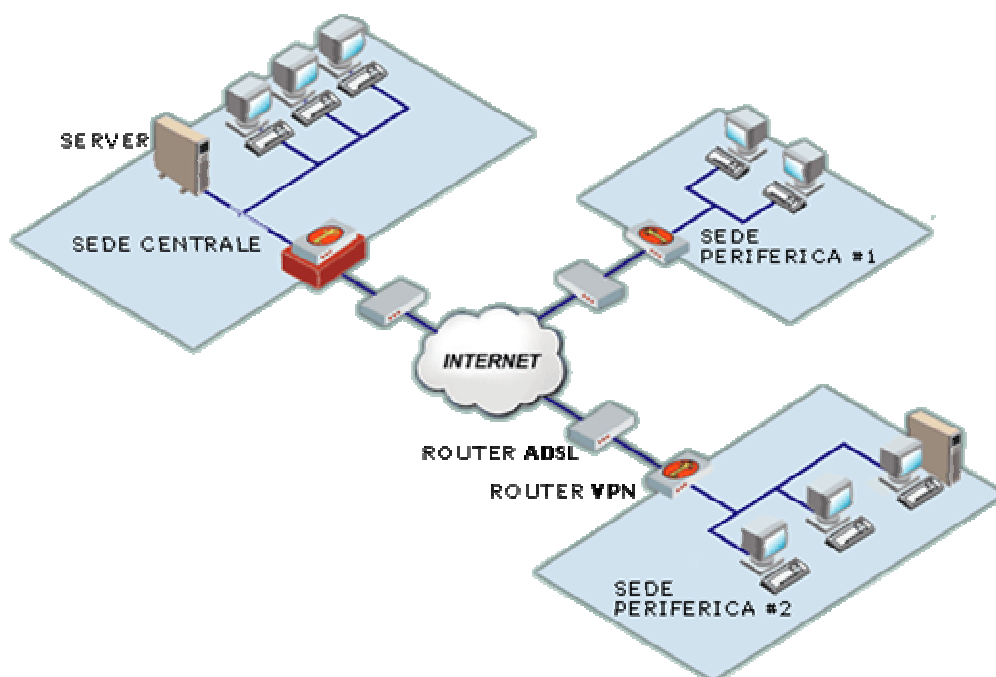



Figura 16 – Ilustração de uma conexão VPN (NEOMEDIA, 2007).

3.1.5.1. Protocolos Utilizados

Segundo ROSSI & FRANZIN (2000), a VPN pode ser utilizada com os seguintes protocolos:

IPSEC: IPSec é um conjunto de padrões e protocolos para segurança relacionada com VPN sobre uma rede IP, e foi definido pelo grupo de trabalho denominado IP Security (IPSec) do IETF (*Internet Engineering Task Force*). O IPSec especifica os cabeçalhos AH (*Authentication Header*) e ESP (*Encapsulated Security Payload*), que podem se utilizados

independentemente ou em conjunto, de forma que um pocote IPSec poderá apresentar somente um dos cabeçalhos (AH ou ESP) ou os dois cabeçalhos.

PPTP - Point to Point Tunneling Protocol: O PPTP é uma variação do protocolo PPP, que encapsula os pacotes em um túnel IP fim a fim.

L2TP - Level 2 Tunneling Protocol: É um protocolo que faz o tunelamento de PPP utilizando vários protocolos de rede (ex: IP, ATM, etc) sendo utilizado para prover acesso discado a múltiplos protocolos.

SOCKS v5*:* É um protocolo especificado pelo IETF e define como uma aplicação cliente-servidor usando IP e UDP estabelece comunicação através de um servidor Proxy.

3.2. Riscos e Vulnerabilidades

3.2.1. Segurança Física

A segurança física de uma rede sem fio, muitas vezes não é lembrada e nem levada em consideração em muitos casos de implementação. Em uma rede cabeada, é um ponto importante que faz necessário a preocupação, e na rede sem fio não é diferente, pois a área de abrangência "física" aumenta substancialmente. Na rede cabeada, a segurança é feita configurando-se uma porta de entrada para a rede (um servidor de autenticação) e a necessidade de um ponto de acesso físico para conectar um equipamento (notebook, computador pessoal, e outros). Já agora a preocupação, além destes pontos citados, aumenta no que diz respeito à abrangência do sinal, o seu alcance e por quem será captado, pois este pode alcançar dezenas ou centenas de metros ao redor da empresa, ou onde esteja localizado (RUFINO, 2005).

O posicionamento dos pontos de acesso deve ser minuciosamente estudado, pois é possível que venha a colidir com necessidades essenciais: a velocidade e o desempenho da rede. Um ponto de acesso posicionado em um ponto alto terá um desempenho melhor, pois o sinal ficará mais limpo, possivelmente livre de interferências. Por conseqüência sua abrangência será

maior, abrindo assim possibilidades de interceptações no sinal, facilitando o acesso não autorizado e sofrendo possíveis ataques.

Uma solução para este problema seria regular a potência de transmissão dos sinais emitidos pelos equipamentos de comunicação sem fio, pois este influencia diretamente na distância do sinal emitido. A escolha de um padrão de transmissão (802.11a, 802.11b ou 802.11g, por exemplo) deve ser levada em consideração também, pois os mesmos possuem características próprias de áreas de abrangência.

3.2.2. Configurações de Fábrica

Sempre que uma empresa fabrica determinado produto, ela procura colocar seu produto o mais compatível possível com os dispositivos encontrados atualmente no mercado e também tenta deixar o mais simplificado possível seu método de instalação. Para que isso tenha efeito positivo, o fabricante deixa muitos de seus recursos de segurança desativados, colocando assim em risco muitas redes montadas por administradores com pouca experiência, que por algumas vezes desconhecem ou não sabem como o fazer (RUFINO, 2005).

Um grande exemplo citado por RUFINO (2005), é o nome de usuário e a senha de acesso padrão em dispositivos controladores e também endereçamentos IP (*Internet Protocol* – Protocolo de Internet). Caso estas configurações não sejam trocadas, facilmente poderão sofrer um ataque e poderá fornecer todo o acesso à rede e a quem nela estiver conectada. As informações de fábrica são facilmente encontradas na Internet, pois os mesmos fabricantes disponibilizam os manuais em suas páginas na web, e assim qualquer pessoa pode ter acesso à mesma.

O SSID (*Service Set IDentifier* - Identificador do domínio de serviço) é uma cadeia de 32 caracteres que identifica cada rede sem fio, e também deve ser motivo de preocupação no momento da configuração de um Ponto de Acesso. (SILVA e DUARTE, 2005).

DUARTE (2003) aconselha alterar o SSID e o *broadcast* de SSID, pois um hacker em posse do mesmo, pode se passar por um ponto de acesso e assim invadir as estações clientes ou inundar a rede com pedidos de dissociação.

3.2.3. Localização de Pontos de Acesso

A qualidade e a segurança da rede estão diretamente ligadas ao posicionamento do ponto de acesso de uma rede sem fio dentro de uma pequena empresa, organização, ou até mesmo no meio doméstico. O sinal do ponto de acesso é enviado para diversas direções, e por este motivo que o concentrador e/ou ponto de acesso deve ficar em um local onde abrangerá toda a área necessitada, evitando que o sinal saia de seu perímetro de segurança (RUFINO, 2005).

A figura abaixo mostra um exemplo do posicionamento de um ponto de acesso de rede. Do lado esquerdo da figura, o ponto de acesso se encontra muito próximo à parede, e com isso o sinal atinge uma parte do lado externo do ambiente, criando assim uma vulnerabilidade e possibilitando um acesso não autorizado a rede. Já no lado direito da figura, o ponto de acesso está posicionado ao centro do ambiente, e o sinal fica praticamente todo restrito internamente.

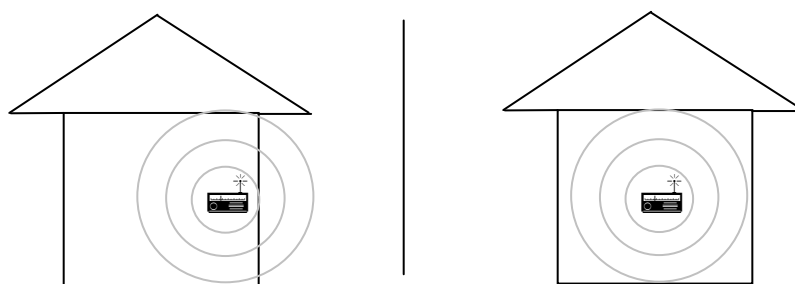



Figura 17 – A posição física do ponto de acesso, grande importância na segurança da rede.

Uma ressalva pode ser feita: o posicionamento do ponto de acesso pode ser considerado como uma tentativa de restringir o sinal, pois não é possível de forma alguma ter um controle sobre ondas eletromagnéticas.

3.2.4. Mapeamento

Este com certeza é uma das primeiras ações que os invasores executam. O invasor tenta conseguir o maior número de informações detalhadas possíveis sobre a rede que está tentando invadir, permitindo que seu ataque seja mais preciso e que sua presença seja com maior dificuldade detectada. Vejamos os dois tipos possíveis de mapeamento:

3.2.4.1. Mapeamento Passivo

Este é um método que é permitido ao atacante mapear os componentes e atividades da rede que se está tentando atacar, com a vantagem de não ser percebido. Uma ferramenta utilizada para fazer este mapeamento é o p0f, que necessita apenas que o intruso esteja dentro da área de sinal do ponto de acesso ou do componente que está transmitindo o sinal, sem a necessidade de comunicar-se com qualquer um. Esta ferramenta fornece informações para que o invasor possa selecionar qual dos dispositivos conectados à rede possivelmente esteja mais vulnerável, sem ser visto, melhorando ainda as chances de conseguir êxito na invasão (RUFINO, 2005, ZALEWSKI, 2007).

A imagem abaixo mostra a execução do programa p0f.

```
jerusalem89998:~/scan28/day1# p0f -s day1.log | egrep 192.168.100.28
p0f: passive os fingerprinting utility, version 1.8.3
(C) Michal Zalewski <lcamtuf@gis.net>, William Stearns <wstearns@pobox.com>
p0f: file: '/etc/p0f.fp', 207 fprints, iface: 'eth0', rule: 'all'.
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28: UNKNOWN [24820:64:2104:1:-1:1:1:48].
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28: UNKNOWN [24820:64:55368:1:-1:1:1:48].
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
192.168.100.28 [1 hops]: SunOS 5.8
```

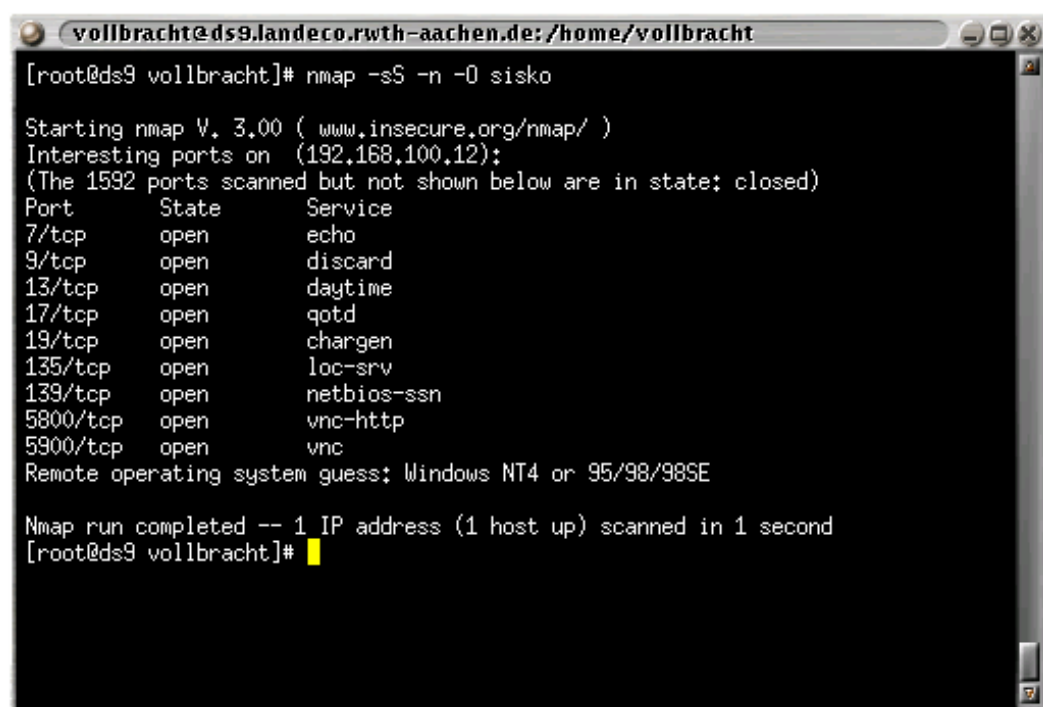



Figura 18 - – O programa p0f em execução (HONEYNET, 2007).

3.2.4.2. Mapeamento Ativo

Com este tipo de mapeamento é possível identificar os equipamentos que estão atuando na rede, bem como seu endereço MAC, sendo suficiente para que, caso haja algum tipo de vulnerabilidade conhecida, ser usada pelo invasor para conseguir invadir a rede (RUFINO, 2005).

Um programa que pode ser usado para realizar o mapeamento ativo é o *TCH-rut*, que permite identificar os endereços MAC em uso pelos dispositivos, bem como o fabricante do mesmo. Porém para que isso seja possível, o atacante já deverá estar participando da rede. Após ter reconhecido e escolhido algum alvo na rede, o atacante parte agora para o ataque direto a ele, utilizando outras ferramentas combinadas, ou isoladamente, como por exemplo, o NMAP (*Network Mapper* - Mapeador de Rede), que verifica quais os serviços que estão ativos no momento, efetuando a varredura das portas abertas no alvo a ser atacado (RUFINO, 2005, INSECURE, 2004).

```
vollbracht@ds9.landeco.rwth-aachen.de:/home/vollbracht
[root@ds9 vollbracht]# nmap -sS -n -O sisko

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on  (192.168.100.12):
(The 1592 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
17/tcp     open        qotd
19/tcp     open        chargen
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
5800/tcp   open        vnc-http
5900/tcp   open        vnc
Remote operating system guess: Windows NT4 or 95/98/98SE

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
[root@ds9 vollbracht]#
```

Figura 19 – NMAP mostrando as portas abertas e os serviços ativos (LINUXUSER, 2005).

Outro programa que pode ser usado para varredura, possui uma *interface* amigável, chamado de *Cheops-ng*, que é capaz de determinar qual sistema operacional está sendo utilizado pela máquina alvo, tipo e modelo (no caso de roteadores, switchs, hubs, etc.), quais os serviços estão em uso no momento entre outros (RUFINO, 2005).

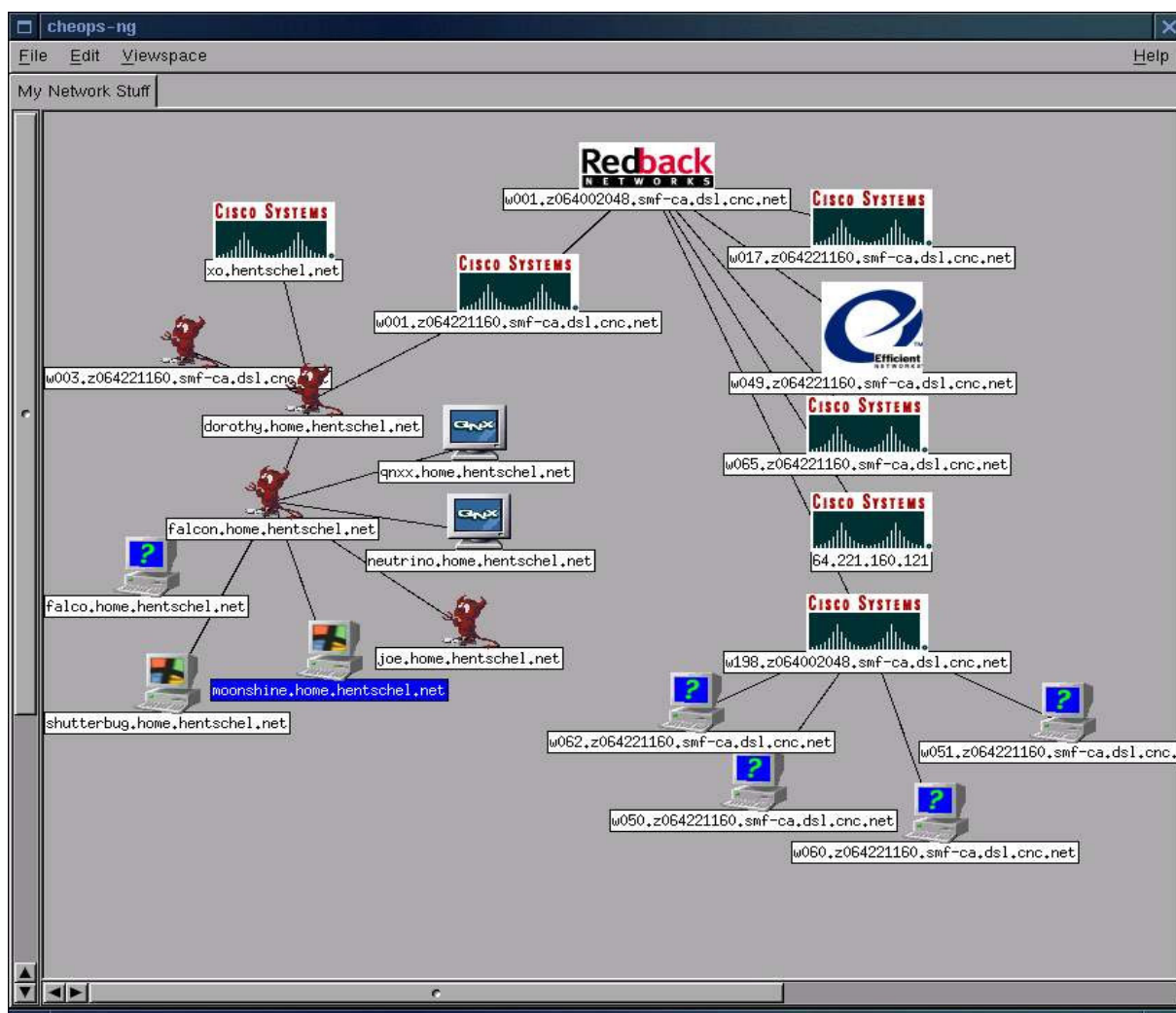



Figura 20 – Cheops-ng com informações detalhadas de seus componentes (CHEOPS-NG, 2007).

3.2.4.3. Geração de Mapas

Essa é uma das possibilidades atualmente disponíveis para criação de áreas de identificação de redes sem fio, através do mapeamento feito por GPS (*Global Positioning System*). Os mapas gerados por GPS possuem uma grande precisão, e podem mostrar qual a área de atuação das redes sem fio, encontrar redes de grande interesse, inclusive quais não estão utilizando WEP ou até mesmo de um órgão ou empresa específica, promover estatísticas de aumento ou diminuição na quantidade de redes sem fio e até os padrões de segurança adotados por elas (DUARTE, 2003).

O GPS Daemon é um software que pode ser integrado a maioria dos GPS existentes hoje no mercado atual. Com esta combinação pode-se obter todas as informações já citadas anteriormente associando mais um software ao processo, o *Kismet*, possibilitando também inserir informações de coordenadas das redes sem fio existentes, gerando com mais detalhes os mapas (RUFINO, 2005, KERSHAW, 2007).

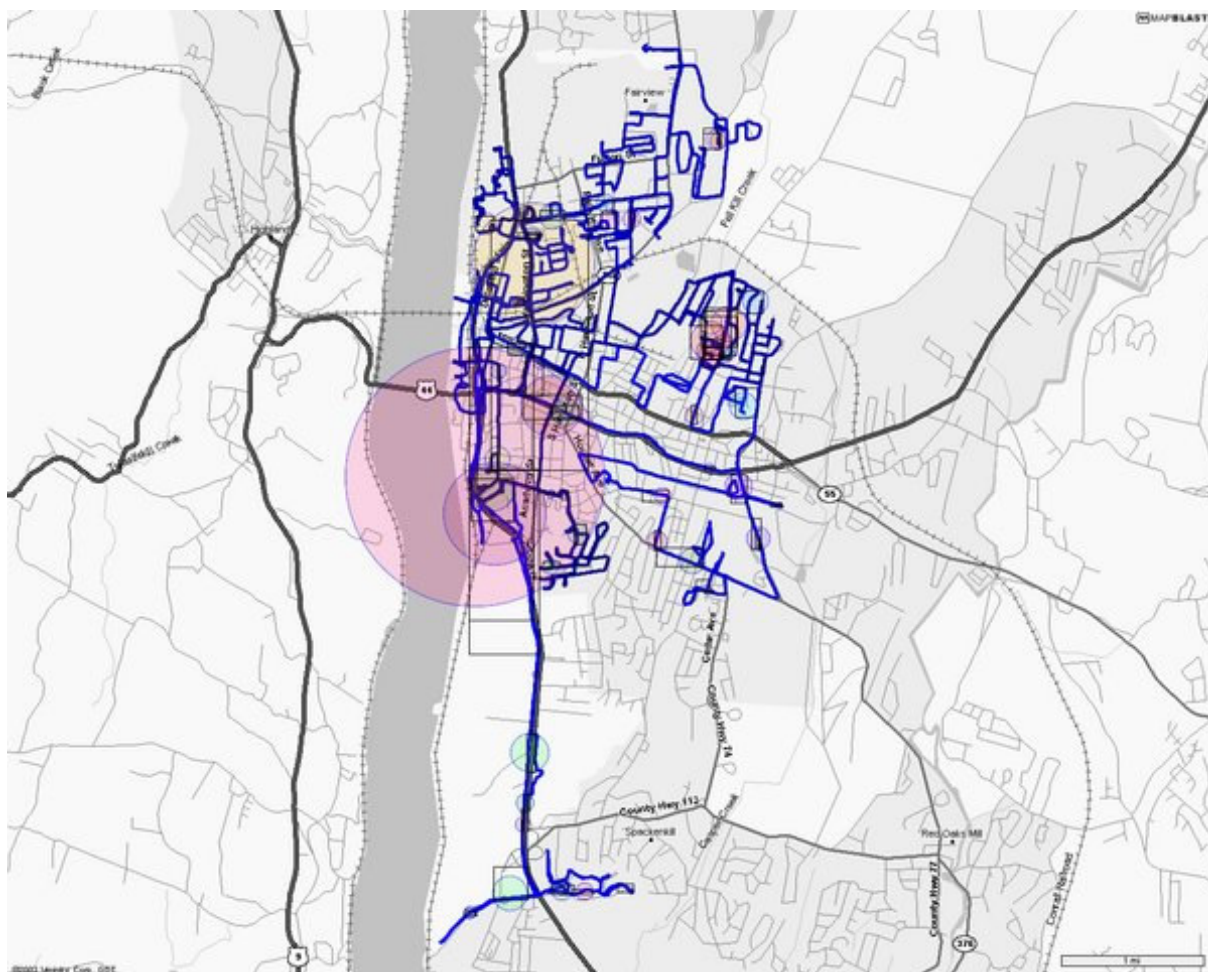



Figura 21 – Mapa gerado pelo Kismet, mostrando redes sem fios disponíveis e sua abrangência (KISMETWIRELESS, 2005).

3.2.5. Vulnerabilidades de Protocolos

3.2.5.1. WEP

A principal falha existente no protocolo WEP é a possibilidade de quebrar seu algoritmo, e muitos dos utilizadores (Administradores de

redes, técnicos, etc...) deste protocolo o condenaram sem entender em que circunstâncias exatas isso pode ocorrer. O protocolo WEP necessita obrigatoriamente que em ambos os lados da comunicação os dispositivos conheçam a chave para cifrar e decifrar, e esse é o grande problema, pois muitas pessoas terão que saber esta chave, principalmente se for um ambiente muito amplo ou com grande mobilidade. Por mais segura que seja a distribuição desta chave, esta será menos secreta, visto que muitas pessoas saberão dela, e que equipamentos e dispositivos possam ser atacados, compartilhados e até roubados (RUFINO, 2005).

O WEP utiliza um vetor de inicialização para impedir a repetição da chave com freqüência, porém como este possui apenas um tamanho de 24 bits, seu período sem repetição fica restrito ao número de pacotes que são enviados e recebidos na transmissão. “Por exemplo, em uma rede onde o AP envia pacotes de 1500 bytes a 11 Mbps ocorrerão repetições a cada: (1500*8)*(2^24)/(11*10^6) @ 18000 segundos, ou seja, a cada 5 horas. Com estas repetições é possível que o atacante realize operações de análise estatística dos quadros cifrados com a mesma chave” (PERES e WEBER, 2004:05)

Outra grande falha do WEP quando utilizando uma autenticação do tipo *Shared Key*, é a possibilidade de um atacante poder alterar um bit da mensagem cifrada sem a necessidade de conhecer seu conteúdo, o segredo compartilhado ou a chave. A utilização do CRC-32 é falha também por ser linear, e com isso o atacante pode identificar os bits do CRC, alterar qualquer outro bit na mensagem e recalcular o checksum para que seja aceito pelos demais dispositivos da rede. (PERES e WEBER, 2004)

3.2.5.2. WPA

Apesar de o protocolo WPA possuir características de segurança superiores ao WEP, também está sujeito a ataques de força bruta ou dicionário, onde o elemento atacante testa uma seqüência de senhas ou

palavras comuns. Uma senha com menos de 20 caracteres é mais fácil de ser quebrada caso esteja utilizando esse protocolo. Conforme citado no tópico 3.2.2, os fabricantes de dispositivos comumente deixam por padrão senhas de 8 à 10 caracteres supondo que o administrador irá alterá-la assim que configurar o mesmo, colocando assim em risco sua rede e expondo a mesma a ataques e invasores. Atualmente existem poucas ferramentas públicas disponíveis para os ataques sob o protocolo WPA, mas podemos citar o WPAcrack, que é utilizado na plataforma Linux através de ataque de dicionário e/ou de força bruta (RUFINO, 2005).

O WPA também pode sofre um ataque do tipo DoS, pois esta vulnerabilidade está ligada diretamente ao algoritmo de garantia da integridade (SILVA, 2005).

Segundo MOSKOWITZ (2003), o algoritmo Michael possui um mecanismo de defesa que ao receber repetidamente mais de uma requisição da mesma origem, ele desativa temporariamente sua operação. Este tipo de defesa foi criado para eliminar os ataques de mapeamento e força bruta. Para isto, basta apenas que o atacante envie dois pacotes a cada minuto, deixando o sistema permanentemente desativado e a detecção do invasor acaba ficando quase impossível, visto que a quantidade de pacotes enviados é pouca, comparando-se aos ataques DoS conhecidos.

3.2.6. Problemas com Redes Mistas

Todo administrador de rede já passou ou irá passar por esta fase de projeto e implementação. Uma rede mista é quando existem dois métodos de acesso a uma rede, podendo ela, por exemplo, ser cabeada e sem fio.

No momento que é decidido agregar uma rede sem fio a uma rede cabeada, deve-se tomar alguns cuidados, pois uma implementação mal feita de uma rede sem fio, irá colocar com certeza em risco a segurança de uma

rede cabeada que foi totalmente planejada, instalada e configurada. Muitas empresas fazem grandes investimentos na área de segurança de redes, contratam profissionais, compram equipamentos, treinam seus funcionários e entre outros, porém através de uma invasão pela rede sem fio, o invasor terá todo acesso à rede cabeada, pois ambas são interligadas e colocará em risco tudo o que foi investido pela empresa.

Abaixo uma figura mostra um exemplo de uma rede mista.

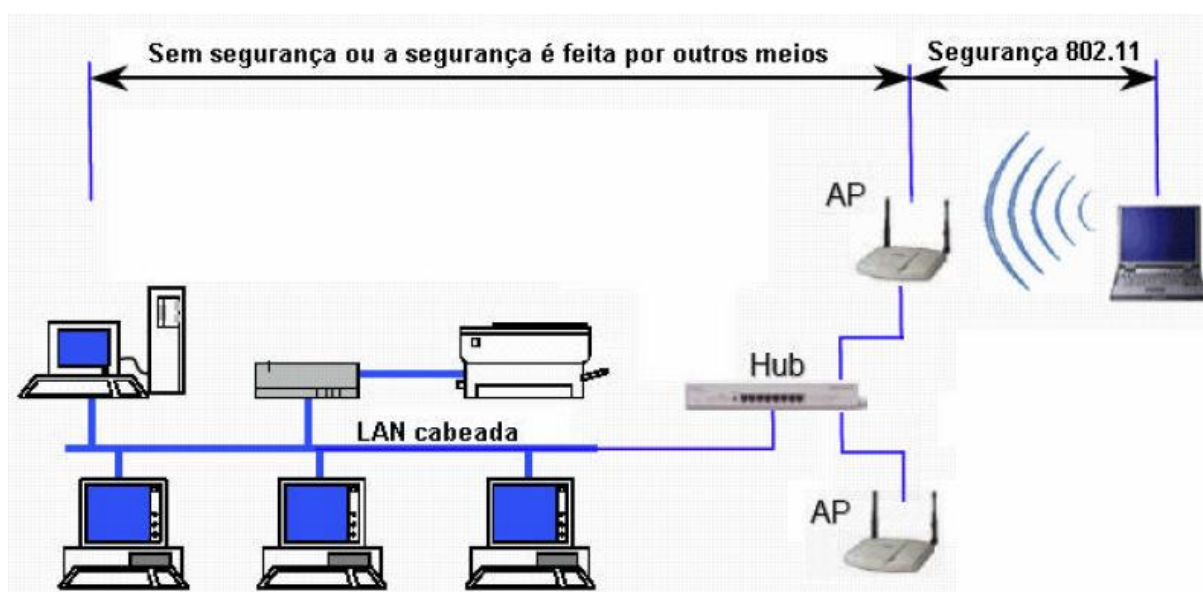



Figura 22 – Exemplo de redes mistas (AMARAL e MAESTRELLI, 2004)

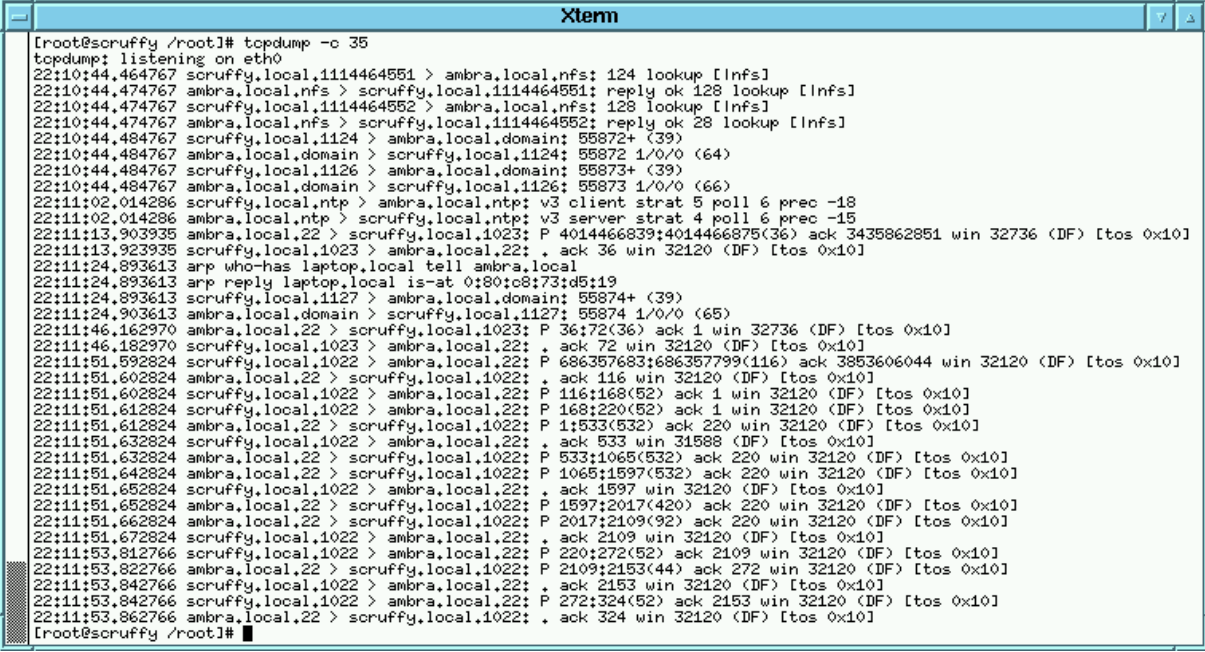
Portanto, aplicar o conceito de segurança em redes sem fio é fundamental quando na junção com uma rede cabeada, evitando assim transtornos para o administrador da rede e para a empresa. Vejamos no tópico seguinte, os principais tipos de ataque a redes sem fio.

3.3. Tipos de Ataque

3.3.1. Escuta de Tráfego

A escuta de tráfego pode ser feita em qualquer tipo de rede, seja ela cabeada ou sem fio, que não esteja utilizando qualquer tipo de cifragem dos

dados para sua transmissão. Ferramentas específicas não são necessárias, é possível utilizar o Tcpdump (ou Windump) que é uma ferramenta tradicional, capaz de colher muitas informações do tráfego de uma rede (RUFINO, 2005)..

Estas ferramentas, assim como outras existentes, são também conhecidas como *Sniffers*, as quais possuem funções maléficas ou benéficas. As benéficas auxiliam a analisar o tráfego da rede e identificar possíveis falhas na rede. As maléficas são utilizadas para capturar senhas, informações confidenciais de clientes e para abrir brechas na segurança da rede (DIEHL e CELANTE, 2001).

A arquitetura de um *Sniffer* pode ser vista na figura abaixo:

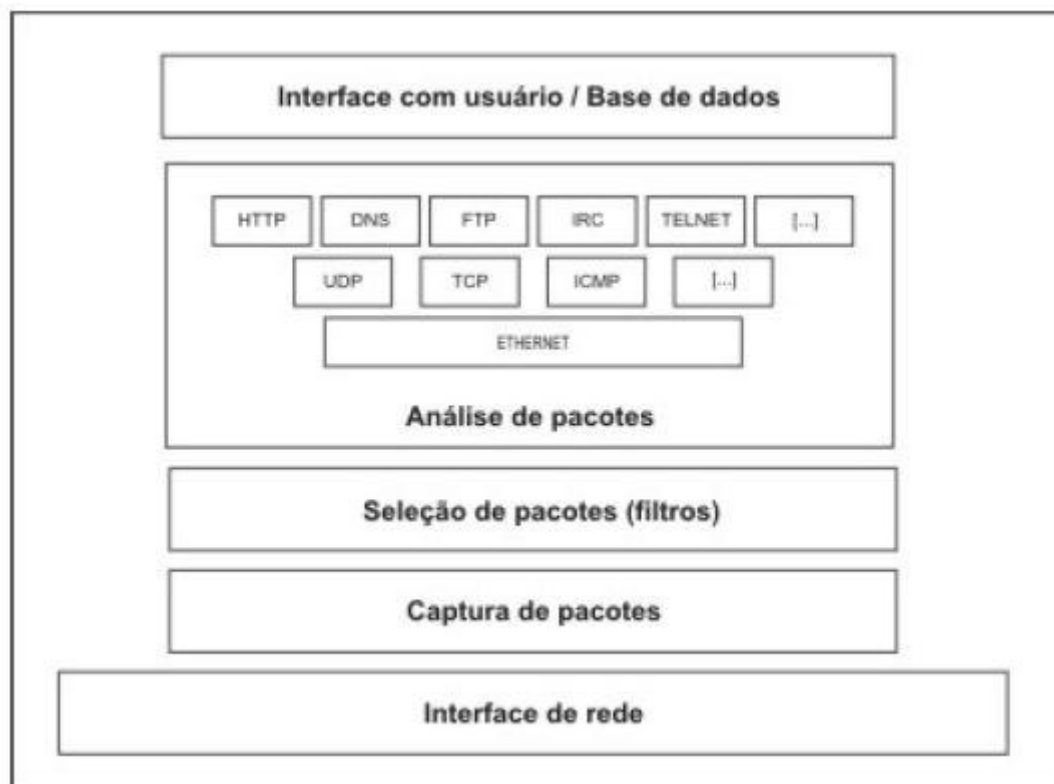



Figura 23 – Arquitetura de um Sniffer (REIS e SOARES, 2002).

Outro comando utilizado é o *ifconfig*, onde este também mostra algumas informações da rede e do dispositivo (endereço MAC, por exemplo). Com o Tcpdump, pode-se obter também o conteúdo que está circulando na rede, como Webmail, POP3/IMAP, entre outros (RUFINO, 2005).

A figura abaixo representa o comando Tcpdump (JACOBSON, LERES e MCCANE, 2005), mostrando várias informações de uma rede.

```
Xterm
[root@scruffy /root]# tcpdump -c 35
tcpdump: listening on eth0
22:10:44.464767 scruffy.local.1114464551 > ambra.local.nfs: 124 lookup [|nfs]
22:10:44.474767 ambra.local.nfs > scruffy.local.1114464551: reply ok 128 lookup [|nfs]
22:10:44.474767 scruffy.local.1114464552 > ambra.local.nfs: 128 lookup [|nfs]
22:10:44.474767 ambra.local.nfs > scruffy.local.1114464552: reply ok 28 lookup [|nfs]
22:10:44.484767 scruffy.local.1124 > ambra.local.domain: 55872+ (39)
22:10:44.484767 ambra.local.domain > scruffy.local.1124: 55872 1/0/0 (64)
22:10:44.484767 scruffy.local.1126 > ambra.local.domain: 55873+ (39)
22:10:44.484767 ambra.local.domain > scruffy.local.1126: 55873 1/0/0 (66)
22:11:02.014286 scruffy.local.ntp > ambra.local.ntp: v3 client strat 5 poll 6 prec -18
22:11:02.014286 ambra.local.ntp > scruffy.local.ntp: v3 server strat 4 poll 6 prec -15
22:11:13.903935 ambra.local.22 > scruffy.local.1023: P 4014466839:4014466875(36) ack 3435862851 win 32736 (DF) [tos 0x10]
22:11:13.923935 scruffy.local.1023 > ambra.local.22: . ack 36 win 32120 (DF) [tos 0x10]
22:11:24.893613 arp who-has laptop.local tell ambra.local
22:11:24.893613 arp reply laptop.local is-at 0:80:c8:73:d5:19
22:11:24.893613 scruffy.local.1127 > ambra.local.domain: 55874+ (39)
22:11:24.903613 ambra.local.domain > scruffy.local.1127: 55874 1/0/0 (65)
22:11:46.162970 ambra.local.22 > scruffy.local.1023: P 36:72(36) ack 1 win 32736 (DF) [tos 0x10]
22:11:46.182970 scruffy.local.1023 > ambra.local.22: . ack 72 win 32120 (DF) [tos 0x10]
22:11:51.592824 scruffy.local.1022 > ambra.local.22: P 686357683:686357799(116) ack 3853606044 win 32120 (DF) [tos 0x10]
22:11:51.602824 ambra.local.22 > scruffy.local.1022: . ack 116 win 32120 (DF) [tos 0x10]
22:11:51.602824 scruffy.local.1022 > ambra.local.22: P 116:168(52) ack 1 win 32120 (DF) [tos 0x10]
22:11:51.612824 scruffy.local.1022 > ambra.local.22: P 168:220(52) ack 1 win 32120 (DF) [tos 0x10]
22:11:51.612824 ambra.local.22 > scruffy.local.1022: P 1:533(532) ack 220 win 32120 (DF) [tos 0x10]
22:11:51.632824 scruffy.local.1022 > ambra.local.22: . ack 533 win 31588 (DF) [tos 0x10]
22:11:51.632824 ambra.local.22 > scruffy.local.1022: P 533:1065(532) ack 220 win 32120 (DF) [tos 0x10]
22:11:51.642824 ambra.local.22 > scruffy.local.1022: P 1065:1597(532) ack 220 win 32120 (DF) [tos 0x10]
22:11:51.652824 scruffy.local.1022 > ambra.local.22: . ack 1597 win 32120 (DF) [tos 0x10]
22:11:51.652824 ambra.local.22 > scruffy.local.1022: P 1597:2017(420) ack 220 win 32120 (DF) [tos 0x10]
22:11:51.662824 ambra.local.22 > scruffy.local.1022: P 2017:2109(92) ack 220 win 32120 (DF) [tos 0x10]
22:11:51.672824 scruffy.local.1022 > ambra.local.22: . ack 2109 win 32120 (DF) [tos 0x10]
22:11:53.812766 scruffy.local.1022 > ambra.local.22: P 220:272(52) ack 2109 win 32120 (DF) [tos 0x10]
22:11:53.822766 ambra.local.22 > scruffy.local.1022: P 2109:2153(44) ack 272 win 32120 (DF) [tos 0x10]
22:11:53.842766 scruffy.local.1022 > ambra.local.22: . ack 2153 win 32120 (DF) [tos 0x10]
22:11:53.842766 scruffy.local.1022 > ambra.local.22: P 272:324(52) ack 2153 win 32120 (DF) [tos 0x10]
22:11:53.862766 ambra.local.22 > scruffy.local.1022: . ack 324 win 32120 (DF) [tos 0x10]
[root@scruffy /root]#
```

Figura 24 – Comando Tcpdump em execução coletando pacotes na rede (CSE UNSW, 2005).

3.3.2. Endereçamento MAC

Este tipo de ataque é feito capturando-se o endereço MAC de uma estação da rede sem fio e armazenando-a para possível futura utilização que pode ser feita de duas formas: bloqueando o dispositivo legítimo e utilizando o endereço da mesma na máquina clandestina. A alteração deste endereço é trivial nos sistemas Unix e é facilmente possível em outros sistemas operacionais. A outra forma é quando o dispositivo legítimo está desligado e assim o clandestino acessa a rede como se fosse o legítimo.

3.3.3. Homem-do-Meio (*man-in-the-middle*)

Esta forma de ataque é conhecida por homem do meio por ser feito a um concentrador que está posicionado no meio de uma conexão de rede sem fio. Normalmente este ataque é feito clonando-se um concentrador já

existente ou criando outro para interpor-se aos concentradores oficiais, recebendo assim as conexões dos novos clientes e as informações transmitidas na rede (RUFINO, 2005 – STALLINGS, 1998).

"É baseado num ataque em que o atacante é capaz de ler, inserir e modificar mensagens entre duas entidades sem que estas tenham conhecimento que a sua ligação foi comprometida" (SIMÕES, 2005: 24).

A figura seguinte representa este conceito:

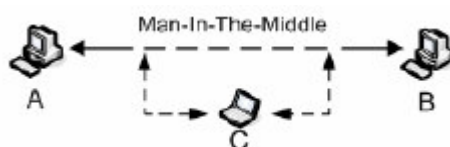



Figura 25 – Exemplo de ataque do tipo homem-do-meio (SIMÕES, 2005).

Conforme o acima exposto, podemos afirmar que nem o cliente A e nem o cliente B possuem conhecimento do elemento invasor C e que este pode interceptar todos os pacotes que são transmitidos naquele meio.

No próximo tópico será mostrado outro método de invasão da rede para a captura de pacotes e invasão da rede sem fio que está utilizando o método WEP para a segurança da mesma.

3.3.4. Quebras de Chaves WEP

Existem diversas formas para que seja quebrada uma chave WEP com diferentes graus de dificuldade e eficiência. Veremos alguns a seguir:

Airsnort: Este tipo de ferramenta é bastante eficaz na quebra de chaves simples, em rede de muito tráfego, porém pouco eficiente devido sua velocidade de quebra. Pode ser usado em conjunto com o Wepcrack, que será visto em seguida. Abaixo uma imagem mostrando uma tela do Airsnort (RUFINO, 2005, DUARTE, 2003).

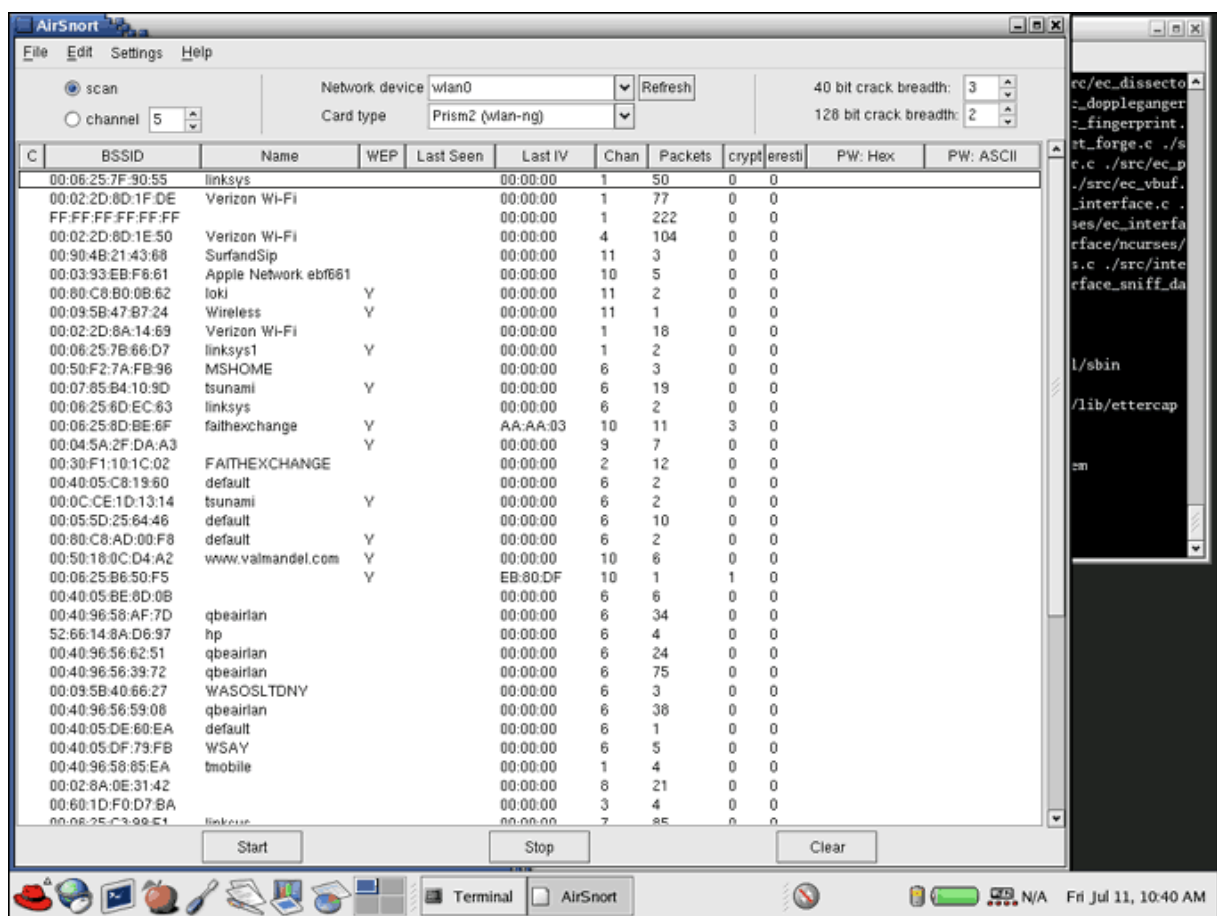
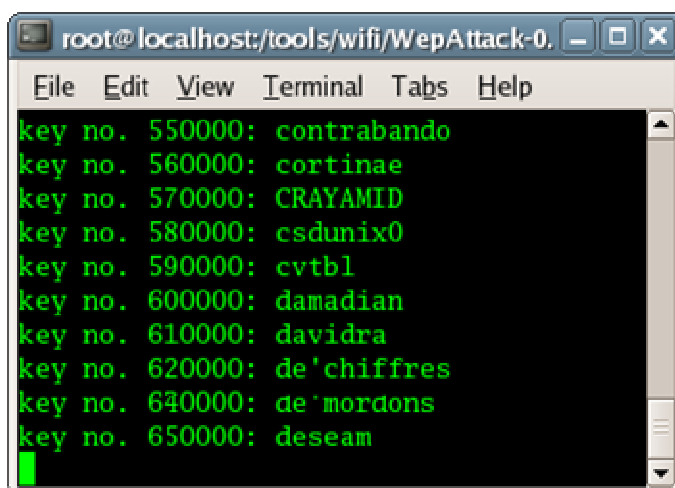



Figura 26 – Programa Airsnort em execução (SECURITYFOCUS, 2007).

Wepcrack: trabalha juntamente com Airsnort, o qual explora as vulnerabilidades do protocolo WEP. Sua principal característica é de ser escrita em Perl, o que indica o seu uso em ambientes multiplataforma (DUARTE, 2003).

```
------------------jc-wepcrack 0.9.6 by Johnny Cache------------------
| Network: 00-30-bd-c0-38-9a     KeySize: 104    Status Running      |
|---------------------------------------------------------------------|
| Total Run Time: 0d 0h 0m 10s    Total Compute Time: 0d 0h 3m 30s   |
| Chunksize: 12    Chunks currently out: 7       Current Stragglers: 0 |
| Percent Complete:  ??        Straggler Threshold:  0d 1h 0m 0s      |
|---------------------------------------------------------------------|
| Next iKey: 00:00:00:00:00:00:00:00:00:00:d3:e0:00:                  |
|---------------------------------------------------------------------|
| Total KeyChunks:         10:00:00:00:00:00:00:00:00:00:00:00:       |
| KeyChunks checked out:  00:00:00:00:00:00:00:00:00:00:0d:51:       |
| KeyChunks checked in:   00:00:00:00:00:00:00:00:00:00:0d:49:       |
|---------------------------------------------------------------------|
```

Figura 27 – Programa Wepcrack em execução (FRESHMEAT, 2007).

Wepattack: Este é um programa opensource desenvolvido para rodas somente em ambiente Linux e seu ataque é baseado na forma do dicionário e pode utilizar qualquer um disponível que contenha informações para a quebra da chave WEP. Sua principal característica é a possibilidade de integrar seu trabalho com outras ferramentas para obter um melhor resultado, como o Tcpdump, o Indump, Ethereal e o famoso John, the ripper (RUFINO, 2005, BLUNK e GIRARDET, 2002).

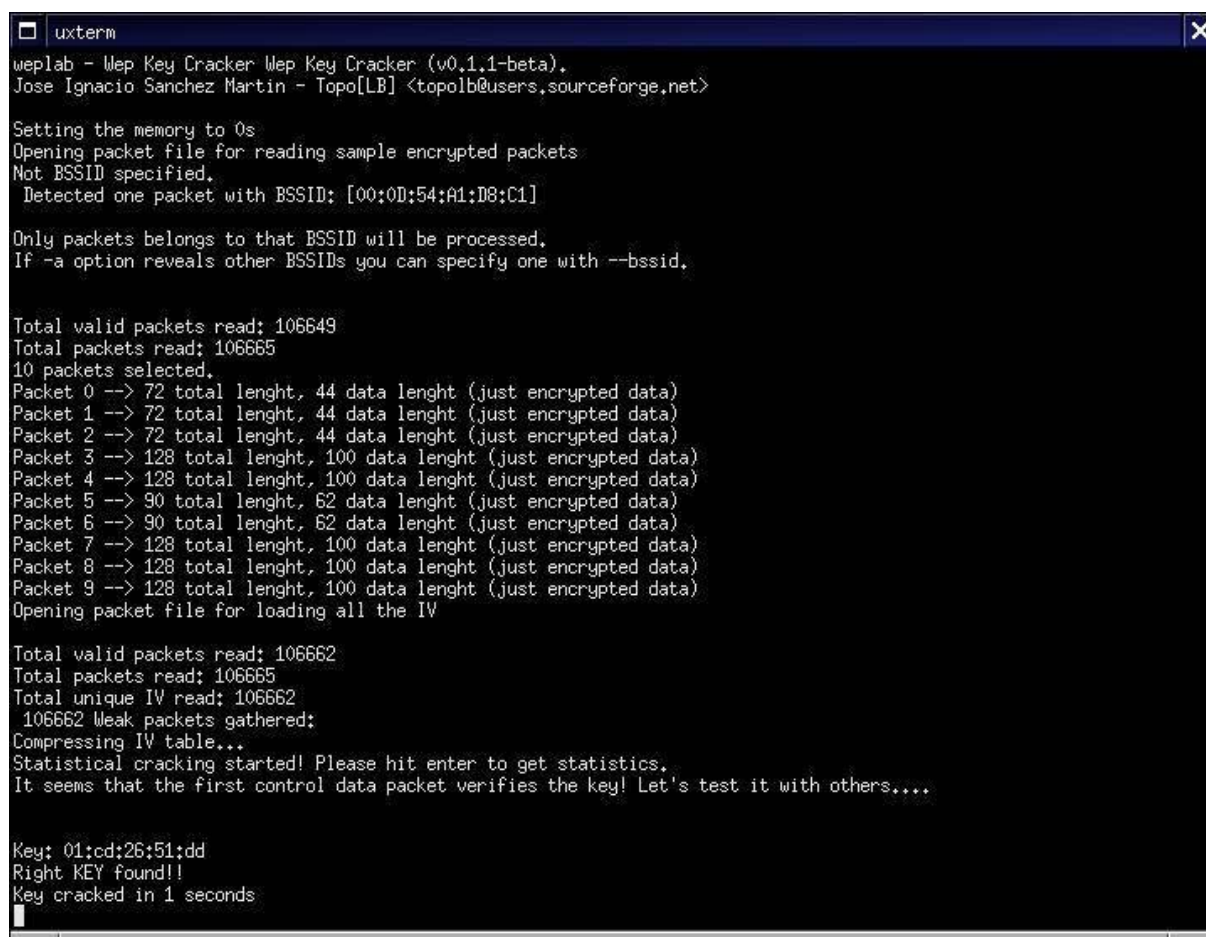



Figura 28 - Programa Wepattack em execução (WIRELESSDEFENCE, 2007).

Weplab: Esta ferramenta utiliza três métodos de ataque. A primeira é baseada no ataque de dicionários, porém ainda não implementada, apenas prevista. A segunda é por meio de força bruta, e a terceira que é o principal método utilizado por esta ferramenta, a de quebra de chaves, onde é feita a análise de falhas na geração de chaves de iniciação. Sua principal característica é a velocidade na quebra da chave WEP, fazendo com que esta ferramenta fosse uma das mais indicadas para este fim até meados de 2004, dando lugar ao próximo método que veremos a seguir, o Aircrack (RUFINO, 2005, MARTÍN, 2004).

Figura 29 – Programa Weplab em execução (LINUXSOFT, 2007)

Aircrack: Como citado no item anterior é considerado uma das ferramentas mais eficientes para quebra de chaves WEP devido sua alta eficiência e seu algoritmo que está sendo incorporado a outros pacotes e ferramentas, com o objetivo de aperfeiçoá-los e melhora-los (RUFINO, 2005).

```
x-terminal-emulator

                           aircrack 2.0

 * Got  569238! unique IVs | fudge factor = 4
 * Elapsed time [00:00:05] | tried 2 keys at 24 k/m

 KB    depth   votes
  0    0/  1   5C(  59) 87(  12) B8(  12) 93(  10) 81(   8) 1F(   5)
  1    0/  2   95( 133) 9B(  52) 56(  25) 33(  13) 55(  13) 58(  12)
  2    0/  1   97( 154) 8F(  20) 41(  13) BB(  13) BC(  13) 25(  12)
  3    0/  1   F3( 182) 1C(  18) EE(  18) 5A(  12) EB(  12) E9(   9)
  4    0/  1   C8( 131) DE(  20) 28(  15) FB(  15) F6(  13) 9C(  11)
  5    0/  1   24( 175) 52(  12) 21(  11) 2B(  11) 57(  11) 78(  11)
  6    0/  6   59(  58) F9(  43) 69(  26) ED(  19) C7(  18) 6B(  15)
  7    0/  8   07(  56) 64(  23) 2E(  22) E8(  22) C2(  19) C5(  19)
  8    0/  2   EA( 120) 4D(  32) 2A(  23) B6(  23) 4C(  20) 7F(  15)
  9    0/  1   71( 142) E0(  26) 8F(  19) 8B(  16) 00(  13) 34(  12)
 10    0/  1   A8( 181) 06(  33) D8(  31) E0(  23) DF(  21) 10(  18)
 11    1/  2   9D( 313) C9( 190) 2A(  85) 71(  79) 54(  75) 29(  71)
 12    0/  1   9D( 162) F1(  23) 17(  21) 1B(  20) A9(  18) 9F(  17)

               KEY FOUND! [5C:95:97:F3:C8:24:59:07:EA:71:A8:9D:9D]

~/aircrack-2.0 $
```

Figura 30 – Programa Aircrack em execução (SOFTONIC, 2007).

3.3.5. Negação de Serviço (DoS – *Denial of Service*)

Este tipo de ataque não necessita que o invasor necessariamente tenha que ter invadido a rede e nem ter acesso à mesma, porém pode causar grandes problemas. Isso ocorre porque os administradores de rede, na maior parte dos casos, se preocupam muito em proteger a rede de invasores e esquecem de colocar nos seus mapas de riscos este tipo de ataque, por imaginar que isso não ocorrerá em suas redes (RUFINO, 2005).

O ataque DoS não visa invadir um computador para extrair informações confidenciais, mas de tornar inacessível os serviços providos pela vítima e usuários legítimos. Nenhum tipo de informação é roubado ou alterado e nem é feito um acesso não autorizado à vítima (MIRKOVIC et al., 2004).

O resultado final de um ataque DoS é a paralisação total ou a reinicialização do serviço ou do sistema do computador da vítima ou ainda o

esgotamento completo dos recursos do sistema, pois estes são limitados e passíveis de serem congelados. É possível ainda ser feito um DDoS (*Distributed DoS*) onde é feito um ataque em massa por vários computadores, ou dispositivos com o mesmo objetivo de parar um ou mais serviços de uma determinada vítima (LAUFER et al., 2005).

3.4. Proposta de implementação de uma Rede Sem fio Segura

A proposta que será exposta agora é para uma utilização em um ambiente coorporativo de pequeno e médio porte, podendo ser também utilizado nas redes domésticas em alguns casos.

Como primeiro passo deverá ser feito um levantamento da estrutura de rede atual para análise de reaproveitamento da própria infra-estrutura e de dispositivos e equipamentos existentes. Uma rede cabeada poderá ser aproveitada agregando-a a rede sem fio criando uma rede mista, ou também como uma possível reserva em casos de falha por diversos motivos da comunicação sem fio.

O posicionamento dos equipamentos responsáveis pela comunicação da rede, os Pontos de Acesso, deverão ser posicionados em locais onde se possa buscar limitar o sinal a um determinado ambiente, como por exemplo, longe de janelas, tentando posicioná-lo o mais próximo do centro da área a ser abrangida.

Alterar as configurações de fábrica em todos os dispositivos é fundamental, como o nome do usuário e a senha para acesso às configurações do Ponto de Acesso, o SSID e o *broadcast* SSID. A potência do Ponto de acesso também poderá ser regulada conforme a necessidade, pois em um ambiente pequeno, como uma sala ou uma seção de 12 ou 15 metros quadrados, por exemplo, onde operam cinco ou seis computadores, não é necessária uma potência alta do sinal de radiofreqüência, pois os dispositivos clientes estarão próximos do ponto de acesso.

A compra dos equipamentos deverá ser de acordo com as necessidades atuais, porém prevendo possíveis mudanças e adaptações futuras, devido a uma necessidade de reestruturação ou evolução da quantidade de clientes que terão acesso à rede. A opção em comprar equipamentos com o padrão 802.11a pode ser

um ponto a mais para a segurança, pois a maioria dos equipamentos existentes utiliza o padrão 802.11b/g. Em contrapartida, o custo com a aquisição dos equipamentos será maior pelo mesmo motivo, de não existir muitos dispositivos, como Notebooks, com o padrão 802.11a já incorporados aos mesmos.

Independente da escolha do padrão para configuração, é necessário que seja feito a proteção da rede com a utilização de mecanismos de segurança. O WEP com criptografia de 128 bits, com uma chave compartilhada é considerado o mínimo para tentar manter a rede livre de intrusos, porém, como já citado no tópico 3.2.5.1, o tempo para que um invasor possa descobrir a chave da rede é pequeno e este poderá ter acesso à mesma em questão de poucas horas.

A utilização do WPA com chave compartilhada é uma configuração intermediária, recomendada para muitas situações, como ambientes domésticos, empresas ou organizações de pequeno porte. Sua segurança é maior que a do WEP, com a vantagem de ter a mesma facilidade de configuração e administração. É recomendada também para médias empresas em que o tráfego das informações não é de caráter confidencial, ou a mesma utiliza conexões do tipo VPN, onde esta protege as informações que circulam na rede, com já visto no tópico 3.1.5.

O protocolo WPA possui outro método de utilização para segurança da rede, o EAP. Dependendo da necessidade e do nível de segurança exigidos pela empresa ou organização, este tipo de segurança é altamente recomendado, pois como citado no tópico 3.1.4.2, necessita de um serviço de autenticação externo como o RADIUS ou a utilização de certificações digitais.

Com estas três linhas de ação apresentadas, é possível afirmar que a configuração ideal depende muito do ambiente em que será aplicada a utilização de redes sem fio, e que o administrador da rede deve sempre estar atento, buscando sempre fazer testes na rede com as ferramentas existentes e as que possivelmente possa surgir, encontrando assim possíveis falhas e soluções para manter a segurança das informações e a confiabilidade no acesso às redes sem fio.

4. CONSIDERAÇÕES FINAIS

4.1. Conclusão

Podemos perceber a grande preocupação das empresas e instituições em aperfeiçoar seus métodos, até então seguros e confiáveis na transmissão das informações, faz com que profissionais da área de administração de redes de computadores procurem aperfeiçoar seus conhecimentos na tecnologia sem fio, para tomar conhecimento de falhas existentes e suas respectivas soluções, como instalação de atualizações ou propondo melhorias nas políticas de segurança da empresa.

Este trabalho teve como objetivo principal estudar melhor as tecnologias existentes em redes sem fio, bem como seus graus de segurança buscando conhecer as falhas existentes e suas possíveis soluções. Os riscos e as vulnerabilidades apresentadas nos capítulos anteriores afetam diretamente toda e qualquer tipo de rede de computadores, resultando algumas vezes em grandes problemas para as empresas. A não observância de medidas de segurança em uma rede é preocupante, pois muitos administradores não possuem conhecimento da amplitude do perigo em que a rede está exposta, possibilitando através destas vulnerabilidades a entrada não autorizada de elementos invasores.

Apesar de todas as medidas de precauções adotadas e que podem ser aplicadas às redes sem fio, sabe-se que a possibilidade de um invasor bem motivado obter sucesso em seu ataque ainda é possível. Com isso, este estudo servirá como material de apoio a administradores de redes, que tenham como filosofia de trabalho, o constante aperfeiçoamento nesta área.

Vale ressaltar que é necessária a incessante busca na melhora das metodologias de segurança, bem como nos padrões adotados, visto que o padrão IEEE 802.11, que é a base para os demais, está constantemente sendo alterado através de grupos de estudo e profissionais de informática, com a finalidade de seu aperfeiçoamento a fim de encontrar uma forma de estabelecer um padrão de segurança aceitável, ideal e confiável.

5. REFERÊNCIAS BIBLIOGRÁFICAS

AIRCRACK. Imagem do programa Aircrack em execução. Acessada em http://screenshots.softonic.com, acessado em 11 de janeiro de 2007.

AIRSNORT. Imagem do programa Airsnort em execução. Acessado em http://www.securityfocus.com, em 11 de janeiro de 2007.

Amaral, Bruno Marques, MAESTRELLI, Marita. **Segurança em Redes Wireless 802.11**. Centro Brasileiro de Pesquisas Físicas - 2004.

Antenas. Imagens representando antenas omni direcional e direcional. Acessado em http://www.qadominicana.com e http://ib.com.br, em 15 de janeiro de 2007.

BEZERRA, Fábio Fernandes. Monografia apresentada como conclusão do curso de Engenheiro de Telecomunicações, assunto: **Ferramenta de Análise Modal de Protocolos de Segurança para Redes Sem Fio**. Universidade Regional de Blumenau, 2004.

BLUNK, Dominik e GIRARDET, Alain. Desenvolvedores do Wepattack. Acessado em http://wepattack.sourceforge.net em 11 de janeiro de 2007.

BOAVIDA, Fernando. **Segurança em Redes 802.11**. Faculdade de Ciências e Tecnologia da Universidade de Coimbra, Portugal - 2004.

CÂMARA, Jéferson e SILVA, Mônica. Trabalho de Conclusão de Curso apresentado para obtenção do grau de Bacharel em Ciência da Computação, assunto: **Redes Sem Fio Metropolitanas Baseadas no Padrão 802.16: Um Estudo de Caso para Belém**. Universidade Federal do Pará, 2005.

CANSIAN, Adriano Mauro, GRÉGIO, André Ricardo Abed e PALHARES, Carina Tebar. Artigo apresentado na Universidade Estadual Paulista – SP. Assunto:

Falhas em Políticas de Configuração: Uma Análise do Risco para as Redes Sem Fio na Cidade de São Paulo. Universidade Estadual Paulista – SP, 2004.

CHEOPS. Imagem do programa Cheops-ng em execução. Acessado em http://cheops-ng.sourceforge.net, em 11 de janeiro de 2007.

Dispositivos Bluetooth. Imagem representativa de Dispositivos Bluetooth. Acessado em http://www.pctuning.cz, em 18 de dezembro de 2007.

FLEISHMAN, Glenn & ENGST, Adam. **Kit do Iniciante em Redes Sem Fio**. 2ª Edição. Editora Makron Books, 2005.

INSEGURE.org - Site do desenvolvedor do NMAP. Acessado em http://www.insecure.org em 18 de dezembro de 2007.

JACOBSON, Van, LERES, Craig e MCCANNE, Steven. Autores do TCPDump: http://www.tcpdump.org da Universidade da Califórnia em Berkeley – EUA, em 18 de dezembro de 2007.

KERSHAW, Mike. Desenvolvedor do programa Kismet Wireless. Acessado em http://www.kismetwireless.net em 18 de dezembro de 2007.

Kismet. Página do software para usar em combinação com GPS. http://www.kismetwireless.net/ acessado em 22 de dezembro de 2007.

KOBAYASHI, Carlos Yassunori. Monografia sobre **Computação Móvel**. BCC – IME – USP, 2004.

LOUREIRO, Antonio A.F., SADOK, Djamel F.H., MATEUS, Geraldo R., NOGUEIRA, Jos Marcos S., KELNER, Judith. **Minicurso apresentado no Congresso da Sociedade Brasileira de Computação**. Campinas, São Paulo, agosto de 2003.

MARTÍN, José Ignacio Sánchez. Desenvolvedor do Weplab. Acessado em http://weplab.sourceforge.net em 18 de janeiro de 2008.

MOSKOWITZ, Robert, Weakness in Passphrase Choice in WPA Interface, Novembro de 2003. Disponível em http://wifinetnews.com/archives/002452.html. Acessado em 19 de janeiro de 2008.

NMAP. Imagem representativa do programa Nmap. Acessado http://www.linux-user.de em 22 de dezembro de 2007.

ONO, Edson Toshiaki. **Implantação de rede Wireless de Alta Velocidade**. Universidade Federal de Santa Catarina. SC – 2004.

P0f. Imagem ilustrando a execução do programa p0f. Acessado em http://www.honeynet.org, em 21 dezembro de 2007.

PALMELA, Pedro Nuno Lopes; RODRIGUES, António Afonso. **Rede de Infravermelhos a Alta Velocidade**. Universidade de Oveiro. Portugal 2002.

PERES, André; WEBER, Raul Fernando. **Considerações sobre Segurança em Redes Sem Fio**. ULBRA - Universidade Luterana do Brasil, RS - 1999.

Placa PCI WLAN. Imagem representativa de um ponto de acesso. Acessado em http://www.abtron.de, em 01 de fevereiro de 2008.

Ponto de Acesso. Imagem representativa de um ponto de acesso. Acessado em http://www.textusweb.com em 21 de janeiro de 2007.

PRADO, Eduardo. Guia completo do WiMAX. Revista do WiMAX, jun de 2004. Disponível em: http://wirelessbrasil.org/eduardo_prado/revista_wimax/guia.html Acesso em 21 de janeiro de 2007.

REIS, Ademar de Souza Junior e SOARES, Milton Filho. Trabalho de Graduação apresentado ao Curso de Bacharelado em Ciência da Computação, Setor de Ciências Exatas, Universidade Federal do Paraná, assunto: **Um Sistema de Testes para a Detecção Remota de Sniffers em Redes TCP/IP**. Universidade Federal do Paraná – Curitiba - PR, 2002.

ROSSI, Marco Antonio G., FRANZIN Oswaldo. **VPN - Virtual Private Network**. GPr Sistemas/ASP Systems, Agosto – 2000.

RUFINO, Nelson Murilo de O. **Segurança em Redes Sem Fio**. Editora Novatec, 2005.

SILVA, Luiz Antonio F. da, DUARTE, Otto Carlos M. B. **RADIUS em Redes sem Fio**. Universidade Federal do Rio de Janeiro. RJ – 2003.

Stallings, W., Cryptography and Network Security, Prentice Hall, 1998.

Tabela de comparativo entre protocolos. Acessado em http://www.teleco.com.br/ieee802.asp, em 30 de janeiro de 2008.

Tcpdump. Imagem representativa do programa Tcpdump. Acessado em http://www.cse.unsw.edu.au/ em 26 de janeiro 2008.

TORRES, Gabriel. **Redes de Computadores,** Curso Completo. Editora Axcel Books, 2001.

VPN. Imagens ilustrando uma conexão VPN. Acessado em http://www.neomedia.it, em 14 de janeiro de 2008.

WEPATTACK. Imagem do programa Wepattack em execução. Acessado em http://www.wirelessdefence.org, acessado em 21 de dezembro de 2007.

WEPCRACK. Imagem do programa Wepcrack em execução. Acessado em http://freshmeat.net, em 11 de janeiro de 2008.

WEPLAB. Imagem do programa Weplab em execução. Acessada em http://www.linuxsoft.cz, em 01 de fevereiro de 2008.

WMAN. Imagem representantiva de uma WMAN. Acessado em http://www.rennes-wireless.org em 30 de novembro de 2007.

WPAN. Imagem representativa de uma WPAN. Acessado em http://www.comnets.rwth-aachen.de, em 10 de janeiro de 2008.

ZALEWSKI, Michal. Hacker criador do programa p0f para utilização no mapeamento passivo em redes em fio. Site acessado em http://lcamtuf.coredump.cx em 10 de janeiro de 2008.

ZANETTI, Alberto René & GONÇALVES, Leandro de Carvalho. Trabalho apresentado na Pós-Graduação em Ciência da Computação, assunto: **Redes Locais Sem Fio**. Universidade Federal de São Carlos, São Paulo, 2003.